Received: 28 November 2022 | Revised: 15 May 2023 | Accepted: 18 May 2023

DOI: 10.1112/plms.12545

RESEARCH ARTICLE

Proceedings of the London Mathematical Society

On the parity conjecture for abelian surfaces

Vladimir Dokchitser[1] | **Céline Maistret**[2]

[1]Department of Mathematics, University College London, London, UK

[2]School of Mathematics, University of Bristol, Bristol, UK

Correspondence
Céline Maistret, School of Mathematics, University of Bristol, Bristol BS8 1UG, UK.
Email: celine.maistret@bristol.ac.uk

Abstract

Assuming finiteness of the Tate–Shafarevich group, we prove that the Birch–Swinnerton–Dyer conjecture correctly predicts the parity of the rank of semistable principally polarised abelian surfaces. If the surface in question is the Jacobian of a curve, we require that the curve has good ordinary reduction at 2-adic places.

MSC 2020
11G40 (11G10, 14K15, 11G30) (primary)

Contents

1 | INTRODUCTION

1.1 | Main results

The Birch–Swinnerton–Dyer conjecture predicts that the Mordell–Weil rank of an abelian variety A over a number field K is given by the order of vanishing of the L-function $L(A/K, s)$ at $s = 1$. Despite being more than half a century old, there has been little theoretical evidence for the conjecture beyond the case of elliptic curves. The aim of the present article is to show that it correctly predicts the parity of the rank of abelian surfaces, at least if one is willing to assume the finiteness of Tate–Shafarevich groups.

Recall that the functional equation for $L(A/K, s)$ says that this function is essentially either symmetric or antisymmetric around the central point $s = 1$, and, consequently, the sign in the functional equation determines the parity of the order of the zero there. Of course, neither the analytic continuation of the L-function nor its functional equation have been proved. However, part of the conjectural framework specifies that the sign is given by the global root number $w_{A/K} \in \{\pm 1\}$, an invariant that is defined independently of any conjectures. One thus expects that the root number controls the parity of the rank of A/K:

Conjecture 1.1 (Parity conjecture). *For every abelian variety A over a number field K,*

$$(-1)^{\mathrm{rk}(A/K)} = w_{A/K}.$$

Our main result is the following:

Theorem 1.2 (=Theorem 13.5). *The parity conjecture holds for principally polarised abelian surfaces over number fields A/K such that $Ш_{A/K(A[2])}$ has finite 2-, 3- and 5-primary part that are*

- *Jacobians of semistable genus 2 curves with good ordinary reduction at primes above 2, or*
- *semistable, and not isomorphic to the Jacobian of a genus 2 curve.*

We note that the hypothesis at primes above 2 requires the underlying curve, and not merely the Jacobian itself, to have good reduction. By a curve with 'ordinary' reduction, we mean one whose Jacobian has ordinary reduction.

There is a range of results on the parity conjecture in the context of elliptic curves, but the progress for higher dimensional abelian varieties has been rather limited. Previous results only apply to sparse families, for example, [8] requires the abelian variety to admit a suitable K-rational isogeny of degree $p^{\dim A}$, and [26] addresses Jacobians of hyperelliptic curves that have been base-changed from a subfield of index 2.

The proof of the above theorem has two main ingredients. The first is the following reduction step that applies to abelian varieties of arbitrary dimension. Its proof is based on the method of regulator constants of [11, 12] and will be explained in Appendix B.

Theorem 1.3. *Let F/K be a Galois extension of number fields with Galois group G. Let A/K be a semistable principally polarised abelian variety such that $Ш_{A/F}$ is finite. If the parity conjecture holds for A/F^H for all 2-groups $H \leqslant G$, then it holds for A/K.*

The second ingredient is a proof of Theorem 1.2 under the assumption that the degree of the field extension generated by $A[2]$ is a power of 2. More precisely, we establish the '2-parity conjecture' in this case. Without some assumption on the Tate–Shafarevich group, the parity conjecture currently appears to be completely out of reach — indeed, it would give an elementary criterion for predicting the existence of points of infinite order, something that seems to be impossibly difficult already for elliptic curves. However, the version for Selmer groups is more tractable. We will write $\mathrm{rk}_p(A/K)$ for the p^∞-Selmer rank of A, that is, $\mathrm{rk}_p(A/K) = \mathrm{rk}(A/K) + \delta_p$, where δ_p is the multiplicity of $\mathbb{Q}_p/\mathbb{Z}_p$ in the decomposition $Ш_{A/K}[p^\infty] \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{\delta_p} \times (\text{finite})$ and is conjecturally always 0.

Conjecture 1.4 (p-Parity conjecture). *For every abelian variety A over a number field K and for a prime number p,*

$$(-1)^{\mathrm{rk}_p(A/K)} = w_{A/K}.$$

Theorem 1.5 (=Theorem 13.3). *The 2-parity conjecture holds for all principally polarised abelian surfaces over number fields A/K such that $\mathrm{Gal}(K(A[2])/K)$ is a 2-group that are*

- *Jacobians of semistable genus 2 curves with good ordinary reduction at primes above 2, or*
- *not isomorphic to the Jacobian of a genus 2 curve.*

Assuming the finiteness of Tate–Shafarevich groups, the p-parity conjecture clearly implies the parity conjecture. In particular, Theorem 1.2 is a direct consequence of Theorems 1.5 and 1.3 applied to $F = K(A[2])$.

The proof of Theorem 1.5 consists of two parts, outlined in more detail in §1.2 and §1.3 below. The first expresses the parity of the 2^∞-Selmer rank of A/K as a product of some local terms λ_{A/K_v},

$$(-1)^{\mathrm{rk}_2 A/K} = \prod_v \lambda_{A/K_v},$$

analogously to the formula for the global root number as a product of local root numbers $w_{A/K} = \prod w_{A/K_v}$, the products taken over all the places of K. This makes crucial use of a Richelot isogeny on A whose existence is guaranteed by the restriction on $\mathrm{Gal}(K(A[2])/K)$.

The second part is the proof that this expression for the parity of the rank is compatible with root numbers. In other words, that $\lambda_{A/K_v} w_{A/K_v}$ satisfies the product formula

$$\prod_v \lambda_{A/K_v} w_{A/K_v} = 1,$$

which leads to the desired expression $(-1)^{\mathrm{rk}_2 A/K} = w_{A/K}$. This product formula is more delicate than one might expect, because one often has $\lambda_{A/K_v} \neq w_{A/K_v}$. However, rather miraculously, $\lambda_{A/K_v} \in \{\pm 1\}$ always differs from $w_{A/K_v} \in \{\pm 1\}$ at an even number of places v. Conjecture 1.14 below gives an explanation for this phenomenon, by describing an explicit relation between the

two local invariants. The key point of the conjecture is that it reduces the global problem of controlling the parity of 2-Selmer ranks to the purely local one of proving an identity between various invariants of genus 2 curves defined over local fields. We prove this conjecture for all semistable curves with good ordinary reduction at primes above 2 (see Theorem 1.16), which let us deduce the 2-parity result of Theorem 1.5 and hence Theorem 1.2 (see Theorem 1.15). The proof relies on explicit formulas and the study of genus 2 curves over local fields, and occupies a substantial part of the present paper.

We note that recently Docking has managed to prove an analogue of the parity formula $(-1)^{\mathrm{rk}_2 A/K} = \prod \lambda_{A/K_v}$ for Jacobians of curves of genus 3 with $\mathrm{Gal}(K(A[2])/K)$ a 2-group, see [9, Thm. 1.5]. A proof of the product formula $\prod_v \lambda_{A/K_v} w_{A/K_v} = 1$ in his setting, combined with Theorem 1.3 above, would give an analogue of Theorem 1.2 for Jacobians of curves of genus 3.

1.2 | Parity of 2^∞-Selmer ranks of Jacobians of C2D4 curves

The main part of the paper deals with the 2-parity conjecture for principally polarised abelian surfaces A that have $G = \mathrm{Gal}(K(A[2])/K)$ a 2-group. Generically, these surfaces are Jacobians of genus 2 curves $C : y^2 = f(x)$ for polynomials $f(x)$ of degree 6. Moreover, G is precisely $\mathrm{Gal}(f(x))$, so the 2-group condition can be phrased as $\mathrm{Gal}(f(x)) \leqslant C_2 \times D_4$, where D_4 denotes the dihedral group of order 8. We will refer to these as C2D4 curves.

Definition 1.6. A *C2D4 curve* C over a field K is a genus 2 curve $C : y^2 = cf(x)$ with $c \in K^\times$ and $f(x)$ monic of degree 6, together with an embedding $\mathrm{Gal}(f(x)) \subseteq C_2 \times D_4$ as a permutation group on six roots (where C_2 and D_4 act separately on two and four roots in their natural ways).

We can control the parity of the 2^∞-Selmer rank of Jacobians of C2D4 curves using purely local data as follows. The Jacobian $J = \mathrm{Jac}\, C/K$ of a C2D4 curve C admits a canonical Richelot isogeny $\phi : J \to \widehat{J}$ to the Jacobian $\widehat{J}$ of another C2D4 curve $\widehat{C}$ (Richelot dual curve), at least if we ignore an exceptional case when a certain invariant $\Delta = \Delta(C)$ vanishes (Definitions 2.1 and 1.12).

Definition 1.7. For a C2D4 curve C over a local field K, let

$$\lambda_{C/K} = \mu_{C/K}\mu_{\widehat{C}/K} \cdot (-1)^{\dim_{\mathbb{F}_2} \ker \phi|_K - \dim_{\mathbb{F}_2} \mathrm{coker}\, \phi|_K}.$$

Here ϕ is the associated Richelot isogeny, $\widehat{C}$ is the Richelot dual curve, $\ker \phi|_K = J(K)[\phi]$ and $\mathrm{coker}\, \phi|_K = \widehat{J}(K)/\phi(J(K))$ for the two Jacobians $J, \widehat{J}$ and $\mu_{C/K}$ is ± 1 depending on whether C/K is deficient (-1) or not $(+1)$; see Definition 2.3.

Theorem 1.8 (See Theorem 3.2). *Let K be a number field. For every C2D4 curve C/K with $\Delta(C) \neq 0$,*

$$(-1)^{\mathrm{rk}_2 \mathrm{Jac}\, C/K} = \prod_v \lambda_{C/K_v},$$

the product taken over all places of K.

Assuming analytic continuation and the functional equation of $L(J/K, s)$, the decomposition of the global root number as a product of local root numbers, $w_{J/K} = \prod_v w_{J/K_v}$, shows that the

analytic rank of the Jacobian satisfies

$$(-1)^{\mathrm{rk}_{\mathrm{an}}\, J/K} = \prod_v w_{J/K_v}.$$

Thus, the above result can be viewed as a 2^∞-Selmer group analogue of the root number formula for parity of the analytic rank given by the functional equation.

The key point is that λ_{C/K_v} is a purely local invariant. It is usually computable for any given curve (see Remark 3.6). By Theorem 1.8, it can be used to determine the parity of the rank assuming finiteness of Ш$[2^\infty]$, without worrying about its compatibility with the Birch–Swinnerton–Dyer conjecture. Such expressions also have direct consequences for arithmetic, as follows.

Example 1.9. For every C2D4 curve $C/\mathbb{Q}$, the 2^∞-Selmer rank of Jac C/F is even over the field $F = \mathbb{Q}(i, \sqrt{17})$. Indeed, every rational prime splits in $F/\mathbb{Q}$, so each term in the product in Theorem 1.8 appears an even number of times. Here $F/\mathbb{Q}$ can, of course, be replaced by any Galois extension of number fields in which every prime splits into an even number of primes.

Remark 1.10. Theorem 1.8 in fact holds for all genus 2 curves whose Jacobians admit a Richelot isogeny and, more generally, for Jacobians of curves that admit an isogeny ϕ to another Jacobian that satisfies $\phi\phi^t = [2]$, see Theorem 3.2.

1.3 | 2-parity conjecture for C2D4 curves

In view of the parity conjecture, Theorem 1.8 and the root number formula $w_{J/K} = \prod_v w_{J/K_v}$ for the Jacobian J, it is tempting to hope that $\lambda_{C/K_v} = w_{J/K_v}$. This is false! However, whenever C is a C2D4 curve over a *number field*, one finds that λ_{C/K_v} always differs from w_{J/K_v} at an even number of places. Finding a purely local explanation for this phenomenon was the most difficult task of the present project.

Definition 1.11. Let $C : y^2 = cf(x)$ be a C2D4 curve over a field K of characteristic 0. The embedding $\mathrm{Gal}(f(x)) \subset C_2 \times D_4$ gives a factorisation of $f(x)$ into monic quadratics

$$f(x) = r(x)s(x)t(x),$$

where $r(x) \in K[x]$ and $\mathrm{Gal}(\bar{K}/K)$ preserves $\{s(x), t(x)\}$. We write the roots as $\alpha_i, \beta_i \in \bar{K}$, with

$$r(x) = (x-\alpha_1)(x-\beta_1), \qquad s(x) = (x-\alpha_2)(x-\beta_2), \qquad t(x) = (x-\alpha_3)(x-\beta_3).$$

We will refer to this data or, equivalently, to the choice of embedding $\mathrm{Gal}(f(x)) \subset C_2 \times D_4$, as a *C2D4 structure* on a genus 2 curve $y^2 = cf(x)$. A C2D4 curve is *centred* if $\beta_1 = -\alpha_1$. Note that any C2D4 curve is isomorphic to a centred one by the substitution $x \mapsto x - \frac{\alpha_1+\beta_1}{2}$.

Definition 1.12. To a centred C2D4 curve, we assign the following quantities:

$$\Delta = c(-\alpha_1^2(\alpha_2+\beta_2-\alpha_3-\beta_3) + \alpha_2\beta_2(\alpha_3+\beta_3) - \alpha_3\beta_3(\alpha_2+\beta_2)),$$
$$\xi = 2((\alpha_2+\alpha_1)(\beta_2+\alpha_1)(\alpha_3+\alpha_1)(\beta_3+\alpha_1) + (\alpha_2-\alpha_1)(\beta_2-\alpha_1)(\alpha_3-\alpha_1)(\beta_3-\alpha_1)),$$

$$\begin{aligned}
\ell_1 &= \alpha_2+\beta_2-\alpha_3-\beta_3 & \eta_1 &= (\alpha_2-\alpha_3)(\beta_2-\beta_3)+(\beta_2-\alpha_3)(\alpha_2-\beta_3),\\
\ell_2 &= \alpha_3+\beta_3 & \eta_2 &= (\alpha_2-\alpha_1)(\alpha_2+\alpha_1)+(\beta_2-\alpha_1)(\beta_2+\alpha_1),\\
\ell_3 &= \alpha_2+\beta_2 & \eta_3 &= (\alpha_3-\alpha_1)(\alpha_3+\alpha_1)+(\beta_3-\alpha_1)(\beta_3+\alpha_1),\\
\delta_1 &= \alpha_1^2 & \hat\delta_1 &= \tfrac{1}{\Delta^2}(\alpha_2-\beta_3)(\alpha_2-\alpha_3)(\beta_2-\alpha_3)(\beta_2-\beta_3),\\
\delta_2 &= (\alpha_2-\beta_2)^2 & \hat\delta_2 &= 4(\alpha_3+\alpha_1)(\alpha_3-\alpha_1)(\beta_3+\alpha_1)(\beta_3-\alpha_1),\\
\delta_3 &= (\alpha_3-\beta_3)^2 & \hat\delta_3 &= 4(\alpha_2+\alpha_1)(\alpha_2-\alpha_1)(\beta_2+\alpha_1)(\beta_2-\alpha_1).
\end{aligned}$$

If C is not centred and C' is the centred curve corresponding to it by shifting the x-coordinate, we define these quantities for C as being those for C', that is, $\Delta(C)=\Delta(C')$, and so on.

We will also use $\mathcal{P}=\ell_1\ell_2\ell_3\eta_2\eta_3\xi(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2)$, for the purposes of the shorthand expression '$\mathcal{P}\neq 0$'; note that δ_i and $\hat\delta_i$ are always non-zero. Note also that in general the invariants $\Delta,\ell_1,\ell_2,\ell_3,\delta_2,\delta_3,\eta_2,\eta_3,\hat\delta_2$ and $\hat\delta_3$ are not necessarily K-rational.

Definition 1.13. For a C2D4 curve C over a local field K of characteristic 0 with $\mathcal{P},\Delta\neq 0$, we define $E_{C/K}$ as the following product of Hilbert symbols

$$\begin{aligned}
E_{C/K} = {} & (\delta_2+\delta_3,-\ell_1^2\delta_2\delta_3)(\delta_2\eta_2+\delta_3\eta_3,-\ell_1^2\eta_2\eta_3\delta_2\delta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2,-\ell_1^2\eta_2\eta_3\hat\delta_2\hat\delta_3)\\
& (\xi,-\delta_1\hat\delta_2\hat\delta_3)(\eta_2\eta_3,-\delta_2\delta_3\hat\delta_2\hat\delta_3)(c,\delta_1\delta_2\delta_3\hat\delta_2\hat\delta_3)\cdot\begin{cases}(\eta_1,-\delta_2\delta_3\Delta^2\hat\delta_1) & \text{if } \eta_1\neq 0\\ 1 & \text{if } \eta_1=0\end{cases}\\
& (\hat\delta_1,-\tfrac{\ell_1}{\Delta})(\ell_1^2,-\ell_2\ell_3)(2,-\ell_1^2)(\hat\delta_2\hat\delta_3,-2).
\end{aligned}$$

We remark that all individual terms δ_1, $\hat\delta_1$, Δ^2, $\frac{\ell_1}{\Delta}$, ℓ_1^2, η_1, $\ell_2\ell_3$, $\eta_2\eta_3$, ξ, $\delta_2+\delta_3$, $\delta_2\eta_2+\delta_3\eta_3$, $\hat\delta_2\eta_3+\hat\delta_3\eta_2$, $\delta_2\delta_3$ and $\hat\delta_2\hat\delta_3$ lie in K as they are preserved by $C_2\times D_4$.

Conjecture 1.14. *For a C2D4 curve C/K over a local field of characteristic 0 with $\mathcal{P},\Delta\neq 0$,*

$$w_{\operatorname{Jac} C/K}=\lambda_{C/K}\cdot E_{C/K}.$$

The essential property of this description is that it explains why w and λ always differ at an even number of places, since, by the product formula for Hilbert symbols, $\prod_v E_{C/K_v}=1$.

Theorem 1.15. *Let K be a number field. The 2-parity conjecture holds for all C2D4 curves C/K with $\mathcal{P},\Delta\neq 0$ for which Conjecture 1.14 holds for C/K_v for all places v of K.*

Proof. Take the product over all places v of the formula in Conjecture 1.14. The result follows from the root number formula $w_{\operatorname{Jac} C/K}=\prod_v w_{\operatorname{Jac} C/K_v}$, Theorem 1.8 and the product formula. □

We will prove this local formula in a large number of cases:

Theorem 1.16 (=Theorem 12.5). *Conjecture 1.14 holds for all C2D4 curves with $\mathcal{P},\Delta\neq 0$ over Archimedean local fields, all semistable C2D4 curves with $\mathcal{P},\Delta\neq 0$ over finite extensions of $\mathbb{Q}_p$ for odd primes p and all C2D4 curves with $\mathcal{P},\Delta\neq 0$ and good ordinary reduction over finite extensions of $\mathbb{Q}_2$.*

Note that Theorem 1.5 now follows from Theorems 1.15 and 1.16, at least provided $\mathcal{P},\Delta\neq 0$. We will also show that the strange formula of Conjecture 1.14 must hold in the non-semistable case too, in that a counterexample would lead to a counterexample to the parity conjecture:

Theorem 1.17 (=Theorem 13.6). *If the 2-parity conjecture is true for all Jacobians of C2D4 curves over number fields, then Conjecture 1.14 holds for all C2D4 curves with $\mathcal{P}, \Delta \neq 0$ over local fields of characteristic 0.*

Remark 1.18. It would be very interesting to have a conceptual interpretation for $E_{C/K}$. The analogous problem appears to be difficult even in the significantly simpler setting of elliptic curves, see [10, Thm. 4] and [13, Thm. 5.8]. One could probably extend the definition of $E_{C/K}$ to $\mathcal{P} = 0$. However, this seems to require a lengthy case by case analysis which we chose to avoid by picking a good model for C that has $\mathcal{P} \neq 0$ (Lemma 11.17). The case $\eta_1 = 0$ has to be treated separately as this condition is model independent.

Manipulating formal algebraic expressions such as $E_{\hat{C}/K}$ with a computer is not practical: these expressions are enormous and computers cannot simplify Hilbert symbols. However, we made extensive use of computational *data* to find the expression for $E_{C/K}$. Once one finds the right list of invariants I_i, it is not difficult to produce the product expression of $E_{C/K}$: one compiles a large list of C2D4 curves and for each curve, one computes $w_{\mathrm{Jac}\, C/K}$, $\lambda_{C/K}$ and all possible Hilbert symbols (I_i, I_j). One then uses linear algebra to find an expression for $w_{\mathrm{Jac}\, C/K}\lambda_{C/K}$ in terms of these Hilbert symbols. The difficulty is then to find this list of invariants in the first place, the main issue being that Hilbert symbols do not behave sensibly under addition. Classical invariants such as Igusa invariants are not sensitive to Richelot isogenies and some of the local data that determine $w_{\mathrm{Jac}\, C/K}\lambda_{C/K}$. Our invariants carry this information, for example, see proof of Theorem 5.2 and §9.1.

In principle, $w_{\mathrm{Jac}\, C/K}\lambda_{C/K}$ only depends on the Richelot isogeny; in terms of Definition 1.11, it means that it is symmetric in r, s and t. However, there appears to be a barrier to finding a Hilbert symbol expression for $w_{\mathrm{Jac}\, C/K}\lambda_{C/K}$ without breaking this symmetry or the symmetry between C and $\hat{C}$.

We have numerically verified Conjecture 1.14 on all 40441 genus 2 curves currently in the LMFDB whose simplified model is given by a degree 6 polynomial, for all odd primes of tame reduction and for each possible C2D4 structure for which $\mathcal{P}, \Delta \neq 0$ (excluding the small number of cases when Magma failed to return a regular model for $\hat{C}$). In theory, one might be able to prove this conjecture over a specific local field by numerically checking a finite list of curves in the vein of Halberstadt's work on root numbers ([20]). However, the length of the list is likely to be unreasonable.

1.4 | Overview

In §2, we review background material, including the construction of the Richelot dual curve and the theory of clusters of [15], which will allow us to control local invariants of genus 2 curves over completions K_v for primes v of odd residue characteristic.

In §3, we explain how to control the parity of the 2^∞-Selmer rank for Jacobians of curves that admit a suitable isogeny, and prove a general version of Theorem 1.8 (see Theorem 3.2). We also prove a formula for $\lambda_{C/K}$, which converts the kernel-cokernel into Tamagawa numbers and other standard quantities (Theorem 3.2); for example, for curves over finite extension of $\mathbb{Q}_p$ with p odd, it reads $\lambda_{C/K} = \mu_C \mu_{\widehat{C}} (-1)^{\mathrm{ord}_2 c_{J/K}/c_{\widehat{J}/K}}$, where J and $\widehat{J}$ are the two Jacobians.

Sections §4–12 focus on C2D4 curves and form the technical heart of the proof of Theorem 1.5 on the 2-parity conjecture and Theorem 1.16 on Conjecture 1.14, which compares local root numbers to the λ-terms. Roughly, the idea is the following.

First of all, we can work out certain cases by making all the terms in Conjecture 1.14 totally explicit. For example, suppose that $C/\mathbb{Q}_p$ is a C2D4 curve for $p \neq 2$, given by $y^2 = f(x)$ with $f(x) \in \mathbb{Z}_p[x]$ monic, and that $f(x) \bmod p$ has four simple roots $\bar{\alpha}_2, \bar{\beta}_2, \bar{\alpha}_3, \bar{\beta}_3$, and a double root $\bar{\alpha}_1 = \bar{\beta}_1$. The reduced curve has a node, and, analogously to multiplicative reduction on an elliptic curve, the Jacobian has local Tamagawa number $v(\alpha_1 - \beta_1)^2 = v(\delta_1)$ if the node is split, and 1 or 2 (depending on whether $v(\delta_1)$ is odd or even) if the node is non-split. Whether the node is split or non-split turns out to be precisely measured by whether or not ξ is a square in $\mathbb{Q}_p$. An explicit computation of the Richelot dual curve shows that, generically (if $v(\Delta)=0$), its reduction also has a node and its Jacobian's Tamagawa number is $2v(\delta_1)$ or 2 depending again on whether ξ is a square (split node) or not (non-split node). Neither curve here is deficient, so we obtain $\lambda_{C/K} = -1$ unless ξ is a non-square and $v(\delta_1)$ is even, in which case it is $+1$. As for multiplicative reduction on elliptic curves, the local root number in this case is $w_{\mathrm{Jac}\, C/\mathbb{Q}_p} = \pm 1$ depending on whether the node is split (-1) or non-split ($+1$). Finally, generically (!) all the terms apart from δ_1 in the expression for $E_{C/\mathbb{Q}_p}$ are units, so that all the Hilbert symbols are (unit,unit)$= 1$, except for one remaining term (ξ, δ_1). The latter is -1 precisely when ξ is a non-square (non-split node!) and $v(\delta_1)$ is odd. This magically combines to $w = \lambda \cdot E$, as required.

We will work out a number of cases by a similar brute force approach (§8–10); this is often rather more delicate than described above, as we have brushed the non-generic cases (when certain quantities become non-units) under the rug. Unfortunately, there is a myriad of possible reduction types that one would need to address to prove the formula $w = \lambda \cdot E$ in general. Instead, we will use a global-to-local trick to cut down the number of cases to a manageable list (from 938 to 48, in the description used in Theorem 7.1). This is based on the following lemma, which follows directly from Theorem 1.8 and the product formula for Hilbert symbols.

Lemma 1.19. *Let K be a number field and C/K a C2D4 curve with $\mathcal{P}, \Delta \neq 0$ for which the 2-parity conjecture holds. If Conjecture 1.14 holds for C/K_v for all places v of K except possibly one place w, then it also holds for C/K_w.*

Thus, to prove the formula $w = \lambda \cdot E$ of Conjecture 1.14 for C over a local field, we can try to deform it to a suitable curve over a number field. The main difficulty, of course, is that we do not a priori have a supply of C2D4 curves over number fields for which we know the 2-parity conjecture! However, we can bootstrap ourselves by making use of the cases for which we have worked out Conjecture 1.14 using the brute force approach outlined above, and which give us a supply of C2D4 curves over number fields for which the 2-parity conjecture holds. Observe also that the truth of the 2-parity conjecture for a C2D4 curve C is

- independent of the choice of model for C and
- independent of the choice of the C2D4 structure.

This will let us show that Conjecture 1.14 is also independent of the choice of model and the choice of C2D4 structure for curves over local fields.

To make this method work, we need to understand how various quantities behave under a change of model (§6), and to have a way to approximate C2D4 curves over local fields by C2D4 curves over number fields that, moreover, behave well at all other places (§11). In §12, we justify that these tools are enough to prove Conjecture 1.14 in all the cases we claim in Theorem 1.16.

In §13, we tie these results together, deal with the exceptional cases when $\mathcal{P} = 0$, $\Delta = 0$ or the abelian surface is not a Jacobian and prove Theorems 1.2 and 1.5.

Appendix A (by A. Morgan) provides a formula for λ for curves with good ordinary reduction over 2-adic fields. Appendix B (by T. Dokchitser and V. Dokchitser) deals with regulator constants and Theorem 1.3.

2 | NOTATION AND BACKGROUND

2.1 | General notation

Throughout the paper, $\mathrm{rk}_p(A/K)$ will denote the p^∞-Selmer rank of A/K (see Conjecture 1.4) and ϕ^t the dual of a given isogeny ϕ.

For a local field K with residue field k, a curve C/K and an abelian variety A/K, we write

π_K	uniformiser of a local non-archimedean field K
$v(x)$	valuation of $x \in \bar{K}$, normalised so that $v(\pi_K) = 1$
$\lvert x\rvert_K$	normalised absolute value of x so that $\lvert\pi_K\rvert_K = \frac{1}{\lvert k\rvert}$
I_K	inertia subgroup of $\mathrm{Gal}(\bar{K}/K)$
Frob_K	a Frobenius element in $\mathrm{Gal}(\bar{K}/K)$
K^{nr}	maximal unramified extension of K
$c_{A/K}$	Tamagawa number for A/K
$\omega^\circ_{A/K}$	Néron exterior form for A/K
$\frac{\omega}{\omega'}$	scalar $\kappa \in K$ with $\omega = \kappa\omega'$ for exterior forms ω, ω'
$w_{A/K}, w_{C/K}$	local root number of A/K and of $\mathrm{Jac}\, C/K$
$n_{A/\mathbb{R}}, n_{C/\mathbb{R}}$	number of components of $A(\mathbb{R})$ and $C(\mathbb{R})$
$\mu_{C/K}$	1 if C is not deficient, -1 if C is deficient (see Definition 2.3)
$\square$	a non-zero square element in K

We will almost always deal with genus 2 curves $C : y^2 = cf(x)$, where $f(x)$ is monic. For convenience of the reader, we list where some of the definitions associated to C may be found (numbering refers to Definitions and Notations):

C2D4 curve	1.11
$\lambda_{C/K}$	1.7
$E_{C/K}$	1.13
$\mathcal{F}, \mathcal{F}_{C2D4}$	explicit 2-adic families of genus 2 curves, 10.4
$\widehat{C}$	Richelot dual curve of C, 2.1
$r(x), s(x), t(x)$	factorisation of $f(x)$, 1.11
α_i, β_i	roots of $f(x)$, 1.11
$\hat{\alpha}_i, \hat{\beta}_i$	roots of defining polynomial of $\widehat{C}$, 2.1
$\delta_i, \hat{\delta}_i, \eta_i, \xi, \Delta, \ell_i, \mathcal{P}$	terms entering $E_{C/K}$, 1.12
	$\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3$ and a general root, 2.4, 2.5, 2.7
C_m, C_t	models for C for $m \in \mathrm{GL}_2(K)$ and $t \in K$, 6.1, 6.3
M_t	matrix and Möbius map to obtain C_t, 6.3
C close to C'	11.1

We will write $\alpha_i(C)$, $\Delta(C)$, and so on, if we wish to stress which curve we are referring to.

We write D_4 for the dihedral group of order 8 and V_4 for the Klein subgroup of S_4.

Every point on $\mathrm{Jac}\, C$ can be represented by the divisor $[P,Q] = P + Q - \infty^+ - \infty^-$, where $P, Q \in C(\bar{K})$ and $\infty^\pm$ are the points at infinity of C. 2-torsion points are of the form $[(\alpha_i, 0), (\beta_i, 0)]$.

2.2 | Richelot isogenies

Definition 2.1 (Richelot dual curve, see [6] Ch. 10, [3] §4, [31] Ch. 8). For a C2D4 curve $C : y^2 = cr(x)s(x)t(x)$ as in Definition 1.11, with $\ell_1, \ell_2, \ell_3, \Delta \neq 0$, its *Richelot dual curve* $\widehat{C}$ is given by

$$\widehat{C} : y^2 = \frac{\ell_1\ell_2\ell_3}{\Delta}\hat{r}(x)\hat{s}(x)\hat{t}(x),$$

where (writing $r'(x)$ for the derivative of $r(x)$, etc.)

$$\hat{r}(x) = \frac{t(x)s'(x) - s(x)t'(x)}{\ell_1}, \qquad \hat{s}(x) = \frac{r(x)t'(x) - t(x)r'(x)}{\ell_2}, \qquad \hat{t}(x) = \frac{r(x)s'(x) - s(x)r'(x)}{\ell_3}.$$

The curve $\widehat{C}$ is a C2D4 curve; $\hat{r}(x), \hat{s}(x), \hat{t}(x)$ are monic quadratics with discriminants $4\Delta^2\hat{\delta}_1/\ell_1^2$, $\hat{\delta}_2/\ell_2^2$ and $\hat{\delta}_3/\ell_3^2$. We denote the roots of $\hat{r}(x)$ (respectively, $\hat{s}(x), \hat{t}(x)$) by $\hat{\alpha}_1, \hat{\beta}_1$ (respectively, $\hat{\alpha}_2, \hat{\beta}_2$ and $\hat{\alpha}_3, \hat{\beta}_3$).

There is an isogeny $\phi : \mathrm{Jac}\, C \to \mathrm{Jac}\, \widehat{C}$ of degree 4 whose kernel is totally isotropic with respect to the Weil pairing and consists of 0 and the 2-torsion points $[(\alpha_i, 0), (\beta_i, 0)]$. The isogeny satisfies $\phi\phi^t = [2]$.

Remark 2.2. When ℓ_1, ℓ_2 or $\ell_3 = 0$, one can define the Richelot dual curve by the same construction by cancelling the offending terms in the equation for $\widehat{C}$ and the expressions for $\hat{r}, \hat{s}, \hat{t}$.

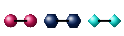
2.3 | Deficiency

Definition 2.3 (Deficiency, [27, Corollary 12]). A curve C of genus g over a local field K is *deficient* if it has no K-rational divisor of degree $g-1$. For a genus 2 curve C/K, being deficient is equivalent to C not having any L-rational points over all extensions L/K of odd degree.

2.4 | Pictorial representation of roots

Notation 2.4. For a C2D4 curve $C : y^2 = cr(x)s(x)t(x)$, we pictorially represent the roots α_1, β_1 of $r(x)$ as **r**uby circles (●), roots α_2, β_2 of $s(x)$ as **s**apphire hexagons (⬢) and roots α_3, β_3 of $t(x)$ as **t**urquoise diamonds (◆). We will sometimes refer to them as ruby, sapphire and turquoise roots, respectively.

Note that the Galois group $\leqslant C_2 \times D_4$ preserves the set of ruby roots and either preserves the set of sapphire roots and the set of turquoise roots, or swaps these two sets around.

Notation 2.5. For a C2D4 curve $C/\mathbb{R}$, it will turn out that most of the local data that we are interested in are encoded in the arrangement of the real roots of the defining polynomial on the real line. We will depict this information by drawing the real roots in the order that they appear in $\mathbb{R}$ and connect two roots r, r' if the points $(r,0)$ and $(r',0)$ are on the same connected component of $C(\mathbb{R})$. Thus, for example, a curve with $\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \alpha_3 < \beta_3$ and $c < 0$ will be depicted by  .

2.5 | Clusters: Curves over local fields with odd residue characteristic

To keep track of the arithmetic of genus 2 curves over p-adic fields with p odd, we will use the machinery of 'clusters' of [15].

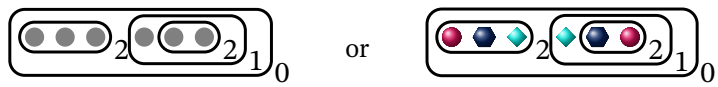
Definition 2.6 (Clusters). Let K be a finite extension of $\mathbb{Q}_p$ and $C : y^2 = cf(x)$ a genus 2 curve, where $f(x) \in K[x]$ is monic of degree 6 with set of roots $\mathcal{R}$. A *cluster* is a non-empty subset $\mathfrak{s} \subset \mathcal{R}$ of the form $\mathfrak{s} = D \cap \mathcal{R}$ for some disc $D = \{x \in \bar{K} \mid v(x-z) \geqslant d\}$ for some $z \in \bar{K}$ and $d \in \mathbb{Q}$.

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

We refer to this data as the *cluster picture* of C.

For C2D4 curves, we will often specify which roots are ruby, sapphire and turquoise: we will refer to this data as the *colouring* of the cluster picture.

Notation 2.7. We draw cluster pictures by drawing roots $r \in \mathcal{R}$ as ●, or as in Notation 2.4 if we wish to specify which root is which, and draw ovals around roots to represent clusters (of size > 1), such as:



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

Definition 2.8 (Twins). A *twin* is a cluster of size 2.

Definition 2.9 (Balanced). A cluster picture of a genus 2 curve is *balanced* if $|\mathcal{R}| = 6$, $d_{\mathcal{R}} = 0$, there are no clusters of size 4 or 5, and there are either no clusters of size 3 or there are two of them, in which case they have equal depth. A curve C is *balanced* if its cluster picture is.

Theorem 2.10. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p with residue field k of size $|k| > 5$. Then every semistable C/K of genus 2 admits a model whose cluster picture is balanced.*

Proof. [15, Cor. 15.3]. □

Lemma 2.11. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p. If C/K is a balanced centred C2D4 curve, then $v(\alpha_i), v(\beta_i) \geqslant 0$ for $i = 1, 2, 3$. Moreover, if $v(\ell_i) = 0$ for some i, then $v(\hat{\alpha}_i), v(\hat{\beta}_i) \geqslant 0$.*

Proof. Since the curve is balanced and centred, $\alpha_1 = -\beta_1$ and the depth of the top cluster is 0. Thus, $v(\alpha_1) = v(\frac{1}{2}(\alpha_1 - \beta_1)) \geqslant 0$. The first claim follows as $v(\alpha_1 - r) \geqslant 0$ for each root r. The second claim follows directly from Definition 2.1, as $\hat{\alpha}_i, \hat{\beta}_i$ are roots of a monic quadratic polynomial with integral coefficients. □

Roughly speaking, the proof of the formula $\lambda = wE$ of Conjecture 1.14 will require a separate computation for each balanced cluster picture.

2.6 | Local invariants of semistable curves of genus 2

Let C/K be a curve of genus 2 over a finite extension of $\mathbb{Q}_p$ for an odd prime p. We record some results of [15] that will let us control the arithmetic invariants of C/K in terms of its cluster picture.

Theorem 2.12 (Semistability criterion, [15, Thm. 1.8]). *Let C/K be a curve of genus 2 over a finite extension of $\mathbb{Q}_p$ for an odd prime p, given by $C : y^2 = cf(x)$ for some $c \in K^\times$ and monic $f(x) \in K[x]$ of degree 6. Then C/K is semistable if and only if the following conditions hold:*

(1) *The extension $K(\mathcal{R})/K$ has ramification degree at most 2.*
(2) *Every cluster $\mathfrak{s}$ with $|\mathfrak{s}| \neq 1$ is I_K-invariant.*
(3) *Every principal cluster $\mathfrak{s}$ has $d_\mathfrak{s} \in \mathbb{Z}$ and $v(c) + |\mathfrak{s}| d_\mathfrak{s} + \sum_{r \notin \mathfrak{s}} v(r - r_\mathfrak{s}) \in 2\mathbb{Z}$, for any (equivalently every) root $r_\mathfrak{s} \in \mathfrak{s}$. Here a cluster $\mathfrak{s}$ is* principal *if $|\mathfrak{s}| \geqslant 3$, $\mathfrak{s}$ does not properly contain a cluster of size 4, and $\mathfrak{s}$ is not a disjoint union of two clusters of size 3 or of sizes 5 and 1.*

We will need to keep track of the analogue of the split/non-split dichotomy for elliptic curves with multiplicative reduction. This is done by keeping track of the Galois action on clusters and associating signs $\pm$ to certain clusters of even size, see [15, Definition 1.13]. We will only need their explicit expressions for balanced pictures:

Definition 2.13 (Sign and $\theta_\mathfrak{s}$). Suppose that C is semistable and balanced.

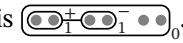
(1) If $\mathcal{R}$ is a union of three twins, the sign of $\mathcal{R}$ is $+$ if $c \in K^{\times 2}$ and $-$ if $c \notin K^{\times 2}$.
(2) Otherwise, for each twin $\mathfrak{s} = \{r_1, r_2\}$, pick a square root $\theta_\mathfrak{s} = \sqrt{c \prod_{r \notin \mathfrak{s}} (\frac{r_1 + r_2}{2} - r)}$ and define its sign $\pm$ through the formula $\frac{\mathrm{Frob}_K(\theta_\mathfrak{s})}{\theta_{\mathrm{Frob}_K(\mathfrak{s})}} \equiv \pm 1$ in the residue field.

Note that the signs depend on the choices of square roots in (2).

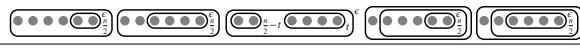
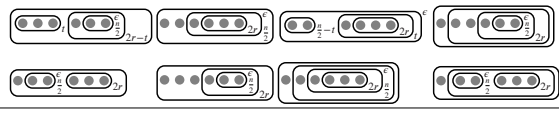
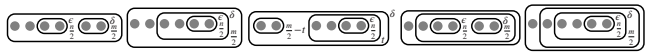
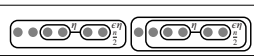
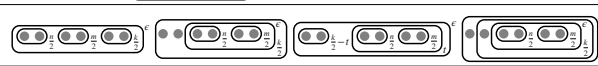
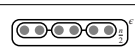
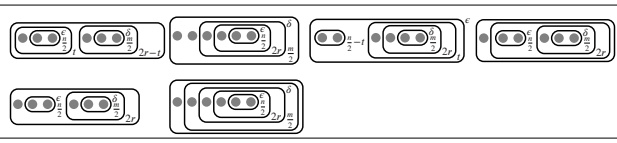
Remark 2.14. When C is semistable and $\mathfrak{s}$ is a twin as in Definition 2.13(2), $v(\theta_\mathfrak{s}^2)$ is always even, equivalently $K(\theta_\mathfrak{s})/K$ is unramified (by Theorem 2.12(3) for $P(\mathfrak{s})$).

Notation 2.15. If we wish to keep track of the signs of clusters in our pictures of Notation 2.7, these will be written as superscripts to the ovals. If we wish to keep track of the Frobenius action,

then lines joining clusters (of size > 1) will indicate that Frobenius permutes them. We refer to cluster pictures with this extra data as *cluster picture with Frobenius action*.

Example 2.16. Let $f(x) = x(x-1)(x-i)(x-i+3)(x+i)(x+i-3)$ over $\mathbb{Q}_3$, where i is a square root of -1. Then there are two clusters of size 2, $\mathfrak{s} = \{i, i+3\}$ and $\mathfrak{s}' = \{-i, -i+3\}$, which are clearly swapped by Frobenius. Here $\theta_{\mathfrak{s}} = \frac{5}{4}\sqrt{1-8i}$ and $\theta_{\mathfrak{s}'} = \frac{5}{4}\sqrt{1+8i}$. Since $\frac{25}{16}(1-8i)$ is not a square in the quadratic unramified extension of $\mathbb{Q}_3$, the two signs are + and − in some order. The cluster picture with Frobenius action is  .

Theorem 2.17 [15, §18, Thms. 18.7, 18.8]. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p, C/K a semistable genus 2 curve and J its Jacobian. Then the cluster picture with Frobenius action of C is one of the ones given in the table below for some integers $n, m, k, r > 0$. The Tamagawa number $c_{J/K}$, deficiency $\mu_{C/K}$ and local root number $w_{C/K}$ are as given in the table. Isomorphic curves have the same type.*

Type		ϵ δ	$c_{J/K}$	$\mu_{C/K}$	$w_{C/K}$
2			1	1	1
$1\times_r 1$			1	1	1
$1\overset{\sim}{\times}_r 1$			1	$(-1)^r$	1
I_n^ϵ		$+$ $-$	n $\tilde{n}$	1 1	-1 1
$1\times_r \mathrm{I}_n^\epsilon$		$+$ $-$	n $\tilde{n}$	1 1	-1 1
$\mathrm{I}_{n,m}^{\epsilon,\delta}$		$+$ $+$ $+$ $-$ $-$ $-$	nm $n\tilde{m}$ $\tilde{n}\tilde{m}$	1 1 1	1 -1 1
$\mathrm{I}_{n\text{-}n}^\epsilon$		$+$ $-$	n $\tilde{n}$	1 1	-1 1
$\mathrm{U}_{n,m,k}^\epsilon$		$+$ $-$	N $\widetilde{\frac{N}{M}} \cdot \widetilde{M}$	1 $(-1)^{nmk}$	1
$\mathrm{U}_{n\text{-}n,k}^\epsilon$		$+$ $-$	$n+2k$ n	1 $(-1)^k$	-1 -1
$\mathrm{U}_{n\text{-}n\text{-}n}^\epsilon$		$+$ $-$	3 1	1 $(-1)^n$	1 1
$\mathrm{I}_n^\epsilon \times_r \mathrm{I}_m^\delta$		$+$ $+$ $+$ $-$ $-$ $-$	nm $n\tilde{m}$ $\tilde{n}\tilde{m}$	1 1 1	1 -1 1
$\mathrm{I}_n^\epsilon \overset{\sim}{\times}_r \mathrm{I}_n$		$+$ $-$	n $\tilde{n}$	$(-1)^r$ $(-1)^r$	-1 1

Notation: Clusters of size 5 and 6 have arbitrary integer depths, $\eta \in \{\pm 1\}$ and $t \in \mathbb{Z}$ are arbitrary. $N = nm + nk + km$, $M = \gcd(n, m, k)$, $\tilde{x} = 2$ if $2|x$ and $\tilde{x} = 1$ if $2 \nmid x$.

We will mostly use this table for balanced curves, that is, the first column of the cluster pictures. Note that type $\mathrm{I}_{n,m}^{\epsilon,\delta}$ is the same as $\mathrm{I}_{m,n}^{\delta,\epsilon}$. Similarly, $\mathrm{I}_n^\epsilon \times_r \mathrm{I}_m^\delta$ is the same as $\mathrm{I}_m^\delta \times_r \mathrm{I}_n^\epsilon$, and $\mathrm{U}_{n,m,k}^\epsilon$ is unchanged by any permutation of the indices.

Remark 2.18. We will use a little more information about the types $\mathrm{I}_{n,m}$ and $\mathrm{I}_n \times \mathrm{I}_m$. Suppose that C has type $\mathrm{I}^{\epsilon,\delta}_{n,m}$ or $\mathrm{I}^{\epsilon}_{n} \times \mathrm{I}^{\delta}_{m}$. Write C_k^+ and C_k^- for the cyclic group C_k on which Frobenius acts trivially and by multiplication by -1, respectively. By [15, Thm. 1.15 and Lemma 2.22], the Néron component group of $\mathrm{Jac}\, C/K^{nr}$ is $\Phi_C = C_n^{\epsilon} \times C_m^{\delta}$. Note also that if C has type $I^{+,-}_{n,m}$ and $\Phi_C = C_k^+ \times C_l^-$, for some even k and l, then necessarily $n = k$ and $m = l$. Indeed, if $C_k^+ \times C_l^- \simeq C_{k'}^+ \times C_{l'}^-$, then $k = k'$ and $l = l'$, since the groups have $2k = 2k'$ Frobenius-invariant elements, and $2l = 2l'$ elements on which Frobenius acts by -1.

3 | PARITY OF 2^∞-SELMER RANK OF JACOBIANS WITH A 2^g-ISOGENY

In this section, we discuss how to control the parity of the 2^∞-Selmer ranks for Jacobians of curves that admit a suitable isogeny.

Definition 3.1. Let C and C' be curves over a local field K whose Jacobians admit an isogeny $\phi : \mathrm{Jac}\, C \to \mathrm{Jac}\, C'$ with $\phi\phi^t = [2]$ (equivalently, an isogeny whose kernel is a maximal isotropic subspace of $\mathrm{Jac}\, C[2]$ with respect to the Weil pairing). We write

$$\lambda_{C/K,\phi} = \mu_{C/K}\mu_{C'/K} \cdot (-1)^{\dim_{\mathbb{F}_2} \ker \phi|_K - \dim_{\mathbb{F}_2} \mathrm{coker}\, \phi|_K},$$

where $\ker \phi|_K = \mathrm{Jac}\, C(K)[\phi]$ and $\mathrm{coker}\, \phi|_K = \mathrm{Jac}\, C'(K)/\phi(\mathrm{Jac}\, C(K))$.

For a C2D4 curve C/K, this is $\lambda_{C/K}$ of Definition 1.7.

3.1 | Parity theorem

Theorem 3.2. *Let C and C' be curves over a number field K whose Jacobians admit an isogeny $\phi : \mathrm{Jac}\, C \to \mathrm{Jac}\, C'$ with $\phi\phi^t = [2]$. Then*

$$(-1)^{\mathrm{rk}_2\, \mathrm{Jac}\, C/K} = \prod_v \lambda_{C/K_v,\phi},$$

the product taken over all places of K.

Proof. Write $A = \mathrm{Jac}\, C$ and $A' = \mathrm{Jac}\, C'$. As in the proof of Thm. 4.3 in [12]

$$2^{\mathrm{rk}_2\, A/K} = \square \cdot \frac{|Ш^{\mathrm{nd}}_{A/K}[2^\infty]|}{|Ш^{\mathrm{nd}}_{A'/K}[2^\infty]|} \cdot \prod_v \frac{|\,\mathrm{coker}\, \phi|_{K_v}|}{|\ker \phi|_{K_v}|},$$

where $Ш^{\mathrm{nd}}_{A/K}$ denotes $Ш_{A/K}$ modulo its divisible part. By a result of Poonen and Stoll ([27, Thm. 8, Cor. 12]), the order of $|Ш^{\mathrm{nd}}_{A/K}|$ is a square if and only if C is deficient at an even number of places, and is twice a square otherwise (and similarly for A'). Hence,

$$2^{\mathrm{rk}_2\, A/K} = \square \cdot \prod_v \frac{\mu_v}{\mu'_v} \cdot \frac{|\,\mathrm{coker}\, \phi|_{K_v}|}{|\ker \phi|_{K_v}|},$$

where $\mu_v = 2$ if C/K_v is deficient and $\mu_v = 1$ otherwise; and similarly for μ'_v. By definition of λ, the 2-adic valuation of the term at v is even if and only if $\lambda_{C/K_v,\phi} = 1$. The result follows. □

3.2 | Kernel/cokernel on local points

Notation 3.3. 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 $A(\mathbb{R})^\circ$ for the connected component of the identity of A and $n_{A/\mathbb{R}} = |A(\mathbb{R})/A(\mathbb{R})^\circ|$ for the number of connected components.

Recall from §2 that when $K/\mathbb{Q}_p$ is a finite extension, $c_{A/K}$ and $\omega^\circ_{A/K}$ denote the Tamagawa number and Néron exterior form for A/K.

Lemma 3.4. *Let C and C' be curves of genus g over a local field K of characteristic 0, whose Jacobians A and A' admit an isogeny $\phi : A \to A'$ with $\phi\phi^t = [2]$. Then*

$$\frac{|\ker\phi|_K|}{|\operatorname{coker}\phi|_K|} = \begin{cases} 2^g & \text{if } K \simeq \mathbb{C}, \\ \left|A(K)^\circ[\phi]\right| \cdot n_{A/K}/n_{A'/K} & \text{if } K \simeq \mathbb{R}, \\ c_{A/K}/c_{A'/K} & \text{if } K/\mathbb{Q}_p \text{ finite, } p \text{ odd}, \\ c_{A/K}/c_{A'/K} \cdot \left|\dfrac{\phi^*\omega^\circ_{A'/K}}{\omega^\circ_{A/K}}\right|_K & \text{if } K/\mathbb{Q}_2 \text{ finite}. \end{cases}$$

Proof. The result if clear for $K \simeq \mathbb{C}$. For $K \simeq \mathbb{R}$, consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)^\circ & \longrightarrow & A(K) & \longrightarrow & A(K)/A(K)^\circ & \longrightarrow & 0 \\ & & \downarrow\phi & & \downarrow\phi & & \downarrow\phi & & \\ 0 & \longrightarrow & A'(K)^\circ & \longrightarrow & A'(K) & \longrightarrow & A'(K)/A'(K)^\circ & \longrightarrow & 0 \end{array}$$

The kernels and cokernels of the vertical maps are finite, so, by the snake lemma,

$$\frac{|\ker\phi|_K|}{|\operatorname{coker}\phi|_K|} = \frac{|\ker\phi|_{A(K)^\circ}|}{|A'(K)^\circ/\phi(A(K)^\circ)|} \cdot \frac{|\ker\phi|_{A(K)/A(K)^\circ}|}{|(A'(K)/A'(K)^\circ)/\phi(A(K)/A(K)^\circ)|}.$$

The map on the connected component of the identity is surjective (as $K \simeq \mathbb{R}$), and the groups of connected components are both finite, so this simplifies to the expression claimed.

The case of non-archimedean K is similar, with $A(K)^\circ$ replaced by $A_1(K)$, the kernel of the reduction on the Néron model of A, see, for example, Lemma 3.8 in [29]. □

Lemma 3.5 [18, Prop. 3.2.2 and 3.3]. *For a smooth projective curve C over $\mathbb{R}$*

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

Remark 3.6. For Jacobians of genus 2 curves over $\mathbb{Q}$, one can compute Tamagawa numbers using van Bommel's algorithm [32, §4.4] and $\frac{|\ker\phi|_{\mathbb{R}}|}{|\operatorname{coker}\phi|_{\mathbb{R}}|}$ is obtained using Lemmata 3.4 and 3.5. Let ω°

and $\hat\omega^\circ$ be Néron exterior forms at $p=2$ for $J=\operatorname{Jac} C$ and $\widehat J=\operatorname{Jac}\widehat C$. The absolute value $|\frac{\phi^*\hat\omega^\circ}{\omega^\circ}|_2$ can be computed as follows. Let $\omega=\frac{dx}{y}\wedge\frac{xdx}{y}$ be an exterior form on J and similarly for $\widehat J$. One has $|\frac{\phi^*\hat\omega}{\omega}|=\frac{\Omega_{\widehat J,\hat\omega}}{\Omega_{J,\omega}}\frac{|\ker\phi|_{\mathbb R}|}{|\operatorname{coker}\phi|_{\mathbb R}|}$ (as in [14, Lemma 7.4]), where the periods Ω can be computed using Magma [2] and $\frac{|\ker|}{|\operatorname{coker}|}$ using Lemma 3.4. Using Magma, we compute $\{\omega_1,\omega_2\}$ a basis of integral differentials at $p=2$. Then a minimal Néron exterior form for J is given by $\omega^\circ=\omega_1\wedge\omega_2$ ([32, §3.2]), which lets us determine $\frac{\omega}{\omega^\circ}$, and similarly for $\widehat J$. Now use

$$\frac{\phi^*\hat\omega^\circ}{\omega^\circ}=\frac{\omega}{\omega^\circ}\cdot\frac{\phi^*\hat\omega}{\omega}\cdot\frac{\phi^*\hat\omega^\circ}{\phi^*\hat\omega}=\frac{\omega}{\omega^\circ}\cdot\frac{\phi^*\hat\omega}{\omega}\cdot\frac{\hat\omega^\circ}{\hat\omega}.$$

3.3 | Odd degree base change

Finally, we record a basic observation regarding the behaviour of Conjecture 1.14 in odd degree unramified extensions.

Lemma 3.7. *Let K be a finite extension of $\mathbb Q_p$ and F/K an unramified extension of odd degree. Let C/K be a C2D4 curve with $\mathcal P,\Delta\neq 0$ and let $A=\operatorname{Jac} C$. Then*

(1) $c_{A/F}=n^2c_{A/K}$ *for some $n\in\mathbb Z$, with $n=1$ if $[F:K]$ is a sufficiently large prime;*
(2) $w_{A/F}=w_{A/K}$*;*
(3) *C/K is deficient if and only if C/F is deficient;*
(4) $E_{C/F}=E_{C/K}$*;*
(5) *Conjecture 1.14 holds for C/K if and only if it holds for C/F.*

Proof.

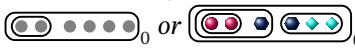
(1) Let Φ be the group of connected components of the special fibre of the Néron model of $A/\mathcal O_K$ with its $\operatorname{Gal}(K^{nr}/K)$-action, so that $c_{A/K}=|\Phi^{\mathrm{Frob}_K}|$ and $c_{A/F}=|\Phi^{\mathrm{Frob}_F}|$. The group Φ carries a perfect symmetric Frob_K-invariant pairing $\Phi\times\Phi\to\mathbb Q/\mathbb Z$ (see [5, 19, Thm. 2.3]). Since Frob_F is an odd power of Frob_K, this forces Φ^{Frob_K} to have a square index in Φ^{Frob_F} (see, e.g. [4, Thm. 2.4.1(ii)] with $f=[F:K]$ and C_k the finite quotient of $\operatorname{Gal}(K^{nr}/K)$ through which the action on Φ factors).
(2) See, for example, [7, Prop. 4.3]. (3) Clear from the definition (see Definition 2.3).
(4) Hilbert symbols are clearly unchanged, and hence, so is $E_{C/K}$.
(5) By (1, 2, 3, 4), the root number, deficiency, E, and the parity of the 2-adic valuation of the Tamagawa numbers are unchanged. Finally, minimal exterior forms are unchanged in unramified extensions, so for 2-adic primes, $|\frac{\phi^*\omega^\circ_{A'/K}}{\omega^\circ_{A/K}}|_F=|\frac{\phi^*\omega^\circ_{A'/K}}{\omega^\circ_{A/K}}|_K^{[F:K]}$ is also unchanged up to squares. The result thus follows from Lemma 3.4. □

4 | MAIN LOCAL THEOREM: BASE CASES

We now turn to the proof of Conjecture 1.14, which relates local root numbers to the local term $\lambda_{C/K}$. As outlined in §1.4, we begin by proving a number of cases through explicit

computation, summarised in Theorem 4.1. The proof will occupy §4–§10. In §11–12, we will deduce the conjecture for the general class of C2D4 curves in Theorem 1.16 by deforming them to number fields and using a global-to-local trick. Recall from §2.4, 2.5 that we draw pictures to indicate the distribution of the roots of $f(x)$ in $\mathbb{R}$ or $\overline{\mathbb{Q}}_p$.

Theorem 4.1. *Let C/K be a C2D4 curve over a local field of characteristic 0, with $\mathcal{P}, \Delta, \eta_1 \neq 0$. Conjecture 1.14 holds for C/K if either*

(1) *$K \cong \mathbb{C}$, or*
(2) *$K \cong \mathbb{R}$, and the picture of C is either*
   -  *or*
   -  *and $\alpha_1 = \bar{\beta}_1$, or*
   -  *and $\alpha_1 = \bar{\beta}_1$, $\alpha_3 = \bar{\beta}_3$, or*
   - *$\alpha_i = \bar{\beta}_i$ for $i = 1, 2, 3$, or*
(3) *$K/\mathbb{Q}_2$ is a finite extension and either*
   - *$C \in \mathcal{F}_{C2D4}$ (see Notation 10.4), or*
   - *C/K has good ordinary reduction, cluster picture*  *with depth of each twin equal to $v(4)$, $f(x) \in \mathcal{O}_K[x]$ with roots in K^{nr}, and $\frac{\delta_2+\delta_3}{16}, \frac{\delta_2\eta_2+\delta_3\eta_3}{32}, \frac{\delta_2\eta_3+\delta_3\eta_2}{8} \in \mathcal{O}_K^\times$, or*
(4) *$K/\mathbb{Q}_p$ is a finite extension for odd p and C is semistable with cluster picture either*
   -  *or*
   -  *with $v(\ell_1) = t$, or*
   -  *with $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$, or*
   -  *with $v(\ell_1) = v(\ell_2) = v(\ell_3) = 0$, or*
   -  *with $v(\ell_1) = \min(n, m)$, $v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$.*

Proof.

(1,2) This follows from Theorems 5.1 and 5.2.
(3) This follows from Theorems 10.5 and 10.3.
(4) A substitution $x \mapsto \pi_K^a x$, $y \mapsto \pi_K^{3a} y$ scales the roots by π_K^a without changing the cluster picture or the leading term c. This does not change any of the Hilbert symbols in $E_{C/K}$ ($\delta_i, \eta_i \ldots$ all have even degree) nor $\lambda_{C/K}$. Thus, we may assume that the depth of the maximal cluster is 0. We may also assume that the C2D4 curve is centred, as a shift in the x-coordinate does not change any of the invariants.

Theorem 7.1 exhausts all possible Frobenius actions on these cluster pictures (after possibly recolouring ). By the semistability criterion (Theorem 2.12), $d_{\mathfrak{s}} \in \mathbb{Z}$ for every cluster $\mathfrak{s}$ of size $\geqslant 3$ and $d_{\mathfrak{t}} \in \frac{1}{2}\mathbb{Z}$ for all twins $\mathfrak{t}$. Moreover, for the cluster pictures  and  , the depth of the twin lies in $\mathbb{Z}$ because $r(x), s(x), t(x) \in K^{nr}[x]$. The result follows from Theorem 7.1. □

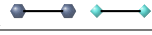
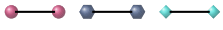
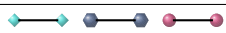
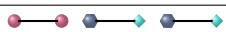
5 | ARCHIMEDEAN PLACES

Theorem 5.1. *Conjecture 1.14 holds for all C2D4 curves over $\mathbb{C}$ with $\mathcal{P}, \Delta \neq 0$.*

Proof. Here $w_{C/\mathbb{C}} = 1$ as C has genus 2, and clearly, $E_{C/K} = 1$ and $\lambda_{C/\mathbb{C}} = (-1)^2 = 1$. □

For curves over $\mathbb{R}$, we shall, for the moment, only prove Conjecture 1.14 in a restricted number of cases. The direct proof below can be extended to all cases (cf. [23]), but we will obtain the remaining ones for free using our methods in §11–12 (see Theorem 12.5).

Theorem 5.2. *Let $C/\mathbb{R}$ be a C2D4 curve with $\mathcal{P}, \Delta, \eta_1 \neq 0$, with Richelot dual curve $\widehat{C}$, Richelot isogeny ϕ and J and $\widehat{J}$ the Jacobians of C and $\widehat{C}$. The table below gives the values of $n_{J/\mathbb{R}}$, $n_{\widehat{J}/\mathbb{R}}$, $|J(\mathbb{R})^\circ[\phi]|$, $\mu_{C/\mathbb{R}}$, $\mu_{\widehat{C}/\mathbb{R}}$, $\lambda_{C/\mathbb{R}}$, $w_{C/\mathbb{R}}$ and $E_{C/\mathbb{R}}$, depending on the roots associated to C and the sign of c. Conjecture 1.14 holds for all curves described in the table.*

	Roots	$n_{J/\mathbb{R}}$	$n_{\widehat{J}/\mathbb{R}}$	$\lvert J(\mathbb{R})^\circ[\phi]\rvert$	$\mu_{C/\mathbb{R}}$	$\mu_{\widehat{C}/\mathbb{R}}$	$\lambda_{C/\mathbb{R}}$	$w_{C/\mathbb{R}}$	$E_{C/\mathbb{R}}$
1	$\alpha_1 = \bar{\beta}_1, \alpha_2 = \bar{\beta}_2, \alpha_3 = \bar{\beta}_3, c > 0$	1	4	4	1	1	1	1	1
2	$\alpha_1 = \bar{\beta}_1, \alpha_2 = \bar{\beta}_2, \alpha_3 = \bar{\beta}_3, c < 0$	1	4	4	−1	1	−1	1	−1
3	$\alpha_1 = \bar{\beta}_1, \alpha_3 = \bar{\beta}_3$ 	1	4	4	1	1	1	1	1
4	$\alpha_1 = \bar{\beta}_1$ 	2	4	4	1	1	−1	1	−1
5		4	4	4	1	1	1	1	1
6		4	4	4	1	1	1	1	1
7		4	4	4	1	1	1	1	1
8		4	2	2	1	1	1	1	1
9		4	4	2	1	1	−1	1	−1

Proof. Write C as $y^2 = cr(x)s(x)t(x)$ as in Definition 1.11. Note that in cases (3)–(9), the picture indicates that $c < 0$. We find that the number of components of $C(\mathbb{R})$ is 0 in case (2), 1 in cases (1, 3), 2 in case (4) and 3 in cases (5)–(9). This gives the values of $n_{J/\mathbb{R}}$ (Lemma 3.5) and $\mu_{C/\mathbb{R}}$ (a curve C of genus 2 is deficient over $\mathbb{R}$ if and only if $C(\mathbb{R}) = \emptyset$, see Definition 2.3).

Recall that $\widehat{C}$ is also a C2D4 curve with equation $y^2 = \frac{\ell_1\ell_2\ell_3}{\Delta}\hat{r}(x)\hat{s}(x)\hat{t}(x)$. From Definitions 1.12 and 2.1, we see that as $r(x), s(x), t(x)$ all have $\mathbb{R}$-coefficients in all the above cases, so do $\hat{r}(x), \hat{s}(x), \hat{t}(x)$. In particular, whether $\hat{\alpha}_i, \hat{\beta}_i$ are real is determined by the sign of the discriminant of the corresponding quadratic. The discriminants of $\hat{r}(x), \hat{s}(x), \hat{t}(x)$ are $\frac{4\Delta^2}{\ell_1^2}\hat{\delta}_1$, $\frac{1}{\ell_2^2}\hat{\delta}_2$ and $\frac{1}{\ell_3^2}\hat{\delta}_3$ (Definition 2.1). Explicitly,

$$(\hat{\alpha}_1 - \hat{\beta}_1)^2 = \frac{4(\alpha_2 - \alpha_3)(\alpha_2 - \beta_3)(\beta_2 - \alpha_3)(\beta_2 - \beta_3)}{(\alpha_2 + \beta_2 - \alpha_3 - \beta_3)^2},$$

with similar expressions for $(\hat{\alpha}_2 - \hat{\beta}_2)^2$ and $(\hat{\alpha}_3 - \hat{\beta}_3)^2$, obtained by permuting the indices 1–3.

If $\alpha_2, \beta_2, \alpha_3, \beta_3 \in \mathbb{R}$, the above discriminant is positive if and only if the roots of the two quadratics are not interlaced (they are 'interlaced' if $\bullet_2 < \bullet_3 < \bullet_2 < \bullet_3$ or vice versa). If either $\alpha_2 = \bar{\beta}_2$ or $\alpha_3 = \bar{\beta}_3$, the discriminant is always positive, being of the form $\frac{z\bar{z}}{w^2}$ for $w \in \mathbb{R}$. An identical analysis applies to $(\hat{\alpha}_2 - \hat{\beta}_2)^2$ and $(\hat{\alpha}_3 - \hat{\beta}_3)^2$.

Putting this information together and considering the sign of the leading term, we deduce that $\hat{C}$ has three real components in all cases above, except for case (8), when it has two real components. This gives the values for $n_{\widehat{J}/\mathbb{R}}$ and $\mu_{\widehat{C}/\mathbb{R}}$ as above for C.

Now consider ϕ-torsion on the connected component of the identity of the Jacobian, $J(\mathbb{R})^\circ[\phi]$. The non-trivial ϕ-torsion points are represented by the divisors $[(\alpha_i, 0), (\beta_i, 0)]$, and the

identity by all pairs of the form $[(x,y),(x,-y)]$. If $\beta_i = \bar{\alpha}_i$, then there is a path on $J(\mathbb{R})$ of the form $[(w,z),(\bar{w},\bar{z})]$ from $[(\alpha_i,0),(\beta_i,0)]$ to the identity (take a path to any $w \in \mathbb{R}$). If $\alpha_i, \beta_i \in \mathbb{R}$ and $(\alpha_i,0)$ and $(\beta_i,0)$ lie on the same component of $C(\mathbb{R})$, then moving $(\beta_i,0)$ to $(\alpha_i,0)$ along $C(\mathbb{R})$ gives a path from $[(\alpha_i,0),(\beta_i,0)]$ to the identity. However, if $\alpha_i, \beta_i \in \mathbb{R}$ and $(\alpha_i,0)$ and $(\beta_i,0)$ do not lie on the same component of $C(\mathbb{R})$, then no such path exist: both points have to remain in $C(\mathbb{R})$ on the path as the x-coordinates will never have the same real part and hence will never be complex conjugate. This fully determines the order of $J(\mathbb{R})^\circ[\phi]$.

The formula for $\lambda_{C/K}$ now follows from Lemma 3.4.

As C has genus 2, the Jacobian is 2-dimensional and $w_{J/\mathbb{R}} = (-1)^{\dim J} = 1$. Conjecture 1.14 for all the cases in the table will thus follow once we justify the formula for $E_{C/\mathbb{R}}$.

We finally turn to $E_{C/\mathbb{R}}$. This will be done by a case-by-case analysis of Hilbert symbols. For convenience, we may assume that the curve is centred, that is, $\alpha_1 = -\beta_1$, as (by definition) this does not affect any of the Hilbert symbols defining $E_{C/\mathbb{R}}$.

Cases 1,2. From their definitions $\ell_1^2, \eta_1, \hat{\delta}_1, \hat{\delta}_2, \hat{\delta}_3 > 0$ and $\delta_1, \delta_2, \delta_3 < 0$. Thus, it follows that $E_{C/\mathbb{R}} = -(\delta_2\eta_2 + \delta_3\eta_3, -\eta_2\eta_3)(\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2, -\eta_2\eta_3) \cdot (\eta_2\eta_3, -1)(c, -1)$. In this case, $\eta_2, \eta_3 \in \mathbb{R}$. If $\eta_2\eta_3 < 0$, then $E_{C/\mathbb{R}} = (c, -1)$. If $\eta_2, \eta_3 > 0$, then $\delta_2\eta_2 + \delta_3\eta_3 < 0$ and $\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2 > 0$ which yields $E_{C/\mathbb{R}} = (c, -1)$. Finally, if $\eta_2, \eta_3 < 0$, then $\delta_2\eta_2 + \delta_3\eta_3 > 0$ and $\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2 < 0$ and $E_{C/\mathbb{R}} = (c, -1)$. Thus, we always have $E_{C/\mathbb{R}} = \mathrm{sign}(c)$, as claimed.

Case 3. Here $\ell_1^2, \Delta^2, \eta_2, \delta_2, \hat{\delta}_1, \hat{\delta}_2, \hat{\delta}_3 > 0$ and $c, \delta_1, \delta_3 < 0$. Hence, $E_{C/\mathbb{R}} = (\delta_2\eta_2 + \delta_3\eta_3, \eta_2\eta_3) \cdot (\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2, -\eta_2\eta_3)$. Either $\eta_3 > 0$ and $\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2 > 0$ so that $E_{C/\mathbb{R}} = 1$, or $\eta_3 < 0$ and $\delta_2\eta_2 + \delta_3\eta_3 > 0$, so that $E_{C/\mathbb{R}} = 1$.

Case 4. Here $\ell_1^2, \Delta^2, \delta_2, \delta_3, \eta_1, \eta_2, \eta_3, \hat{\delta}_1, \hat{\delta}_2, \hat{\delta}_3 > 0$ and $c, \delta_1 < 0$, so that $E_{C/\mathbb{R}} = (\delta_1, c) = -1$.

In the remaining cases $c < 0$ and all roots are real, so $\delta_1, \delta_2, \delta_3, \ell_1^2, \Delta^2 > 0$, and $E_{C/\mathbb{R}} = (\delta_2\eta_2 + \delta_3\eta_3, -\eta_2\eta_3) \cdot (\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2, -\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3)(\xi\eta_2\eta_3, -\hat{\delta}_2\hat{\delta}_3) \cdot (-c, \hat{\delta}_2\hat{\delta}_3)(\eta_1, -\hat{\delta}_1)(\hat{\delta}_1, -\frac{\ell_1}{\Delta})$.

Cases 5,6,7. Here $\eta_1, \eta_2, \eta_3, \xi, \hat{\delta}_1, \hat{\delta}_2, \hat{\delta}_3 > 0$, so that $E_{C/\mathbb{R}} = 1$.

Case 8. Here $\eta_2, \eta_3, \xi, \hat{\delta}_2, \hat{\delta}_3 > 0$ and $\hat{\delta}_1, \ell_1 < 0$, so that $E_{C/\mathbb{R}} = (-1, -\frac{\ell_1}{\Delta})$. Noting that $\Delta = -c((\alpha_1+\beta_2)(\alpha_1-\beta_2)(\alpha_2-\alpha_3) + (\beta_3-\beta_2)((\beta_2-\alpha_1)(\alpha_3-\alpha_2) + (\alpha_2+\alpha_1)(\alpha_3-\alpha_1)))$, it follows that $\Delta > 0$ so that $\frac{\ell_1}{\Delta} < 0$ and $E_{C/\mathbb{R}} = 1$.

Case 9. Here $\eta_2, \eta_3, \xi, \hat{\delta}_1, \hat{\delta}_2, \hat{\delta}_3 > 0$ and $\eta_1 < 0$, so that $E_{C/\mathbb{R}} = -1$. □

6 | CHANGING THE MODEL BY MÖBIUS TRANSFORMATIONS

For the proof of our main results on Conjecture 1.14, it will often be useful to be able to change the model of a C2D4 curve. This does not change the classical arithmetic invariants, but it does affect the terms $\Delta, \xi, \ldots$ that enter $E_{C/K}$ and hence Conjecture 1.14. In this section, we discuss possible changes of model and their effect on these terms.

6.1 | GL_2 action on models

Definition 6.1. Let C be a C2D4 curve over a field K of characteristic 0,

$$C : y^2 = c\prod_{i=1}^{3}(x-\alpha_i)(x-\beta_i),$$

and $m=\left(\begin{smallmatrix}\mathbf{a}&\mathbf{b}\\ \mathbf{c}&\mathbf{d}\end{smallmatrix}\right)\in \mathrm{GL}_2(K)$ such that the associated Möbius map $m(z)=\frac{\mathbf{a}z+\mathbf{b}}{\mathbf{c}z+\mathbf{d}}$ has $m(\alpha_i), m(\beta_i)\neq\infty$. We define the model C_m of C by

$$C_m\ :\ y_m^2 = c_m\prod_{i=1}^{3}(x_m-\alpha_i')(x_m-\beta_i'),$$

with $\alpha_i'=m(\alpha_i)$, $\beta_i'=m(\beta_i)$, $c_m=c\prod_{i=1}^3(\mathbf{c}\alpha_i+\mathbf{d})(\mathbf{c}\beta_i+\mathbf{d})$, via the transformation $x_m=\frac{\mathbf{a}x+\mathbf{b}}{\mathbf{c}x+\mathbf{d}}$ and $y_m = y\cdot\frac{(\mathbf{ad}-\mathbf{bc})^3}{(\mathbf{c}x+\mathbf{d})^3}$. One can check that this construction satisfies $(C_m)_{m'}=C_{m'm}$.

Remark 6.2 (See also [22, §2]). If a genus 2 curve over K admits two hyperelliptic models $C: y^2=cf(x)$ and $C': y_2^2=c_2f_2(x_2)$, then the x-coordinates are always related by a Möbius map $x_2=m(x)=\frac{\mathbf{a}x+\mathbf{b}}{\mathbf{c}x+\mathbf{d}}$ for some $\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in K$ (because these are the only transformations on $\mathbb{P}^1$ that is the quotient of the curve by the hyperelliptic involution). If both equations have degree 6, the model C' then agrees with C_m up to scaling the y-coordinate by a suitable constant, $y_2=\lambda y_m$ for some $\lambda\in K$.

It will be particularly convenient to have a one-parameter family of models.

Definition 6.3. Let K be a field of characteristic 0 and $\alpha_1^2\in K$. For $t\in K\setminus\{\frac{1}{\alpha_1},-\frac{1}{\alpha_1}\}$, define $M_t=\left(\begin{smallmatrix}1&t\alpha_1^2\\ t&1\end{smallmatrix}\right)$ with the corresponding Möbius map over K given by $M_t(z)=\frac{z+t\alpha_1^2}{tz+1}$. Write also $M_\infty=\left(\begin{smallmatrix}0&\alpha_1^2\\ 1&0\end{smallmatrix}\right)$ and $M_\infty(z)=\frac{\alpha_1^2}{z}$.

We will use the shorthand notation $C_t=C_m$ for centred curves $C: y^2=c\prod_{i=1}^3(x-\alpha_i)(x-\beta_i)$. Note that $M_t(\alpha_1)=\alpha_1$ and $M_t(-\alpha_1)=-\alpha_1$, so that C_t is also centred.

Lemma 6.4. *Let M be a Möbius map defined over a field K. Suppose that $\alpha_1^2\in K$ and that $M(\alpha_1)=-M(-\alpha_1)$. Then $M=r\circ M_t$ for some $t\in K\cup\{\infty\}$, where $r(z)=\frac{M(\alpha_1)}{\alpha_1}z$.*

Proof. First note that $\frac{M(\alpha_1)}{\alpha_1}\in K$. Hence, $r^{-1}\circ M$ is defined over K and fixes α_1 and $-\alpha_1$. Now write $r^{-1}\circ M(z)=\frac{\mathbf{a}z+\mathbf{b}}{\mathbf{c}z+\mathbf{d}}$. Since $r^{-1}\circ M(\alpha_1)=\alpha_1$ and $r^{-1}\circ M(-\alpha_1)=-\alpha_1$, we have $\mathbf{a}=\mathbf{d}$ and $\mathbf{b}=\mathbf{c}\alpha_1^2$. If $\mathbf{a}\neq 0$, the map is of the required form. If $\mathbf{a}=0$, then $r^{-1}\circ M(z)=\frac{\alpha_1^2}{z}$, so $M(z)=r\circ M_\infty(z)$. □

6.2 | Rebalancing

Theorem 6.5. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p, with residue field k of size $|k|>5$, and C/K a semistable C2D4 curve. There is $m\in\mathrm{GL}_2(K)$ such that C_m is balanced.*

Proof. Theorem 2.10 and Remark 6.2. □

Theorem 6.6. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p, with residue field k of size $|k|\geqslant 23$. Let C/K be a centred balanced semistable C2D4 curve. Then there is a $t_0\in K$ such that for all $t\in K$ with $v(t-t_0)>0$, the cluster picture of C_t with signs and Frobenius action on proper clusters, its colouring, $v(c)$ and $v(\Delta)$ are the same as that of C and*

- *if the cluster picture of C_t is*  ,  ,  ,  *or*  *then C_t has $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$;*
- *if the cluster picture of C_t is*  *or*  *then C_t has $v(\ell_1) = v(\ell_2) = v(\ell_3) = 0$;*
- *if the cluster picture of C_t is*  *then C_t has $v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ and $v(\ell_1) = \min(n, m)$;*
- *if the cluster picture of C_t is*  *then C_t has $v(\ell_1) = v(\ell_2) = v(\ell_3) = j$.*

Proof. Since C is centred and balanced, all the roots are necessarily integral (Lemma 2.11).

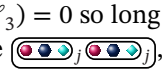
One readily checks that

$$M_t(r_1) - M_t(r_2) = (r_1 - r_2) \cdot \frac{(1 - t^2\alpha_1^2)}{(tr_1 + 1)(tr_2 + 1)}.$$

In particular, so long as $t \not\equiv -1/r_1, -1/r_2, 1/\alpha_1, -1/\alpha_1$ in k, one necessarily has $v(r_1 - r_2) = v(M_t(r_1) - M_t(r_2))$. Thus, if $t \not\equiv -1/r$ in k for any root r, then C_t has the same cluster picture as C, with the same colouring. The Galois action on proper clusters and the signs of clusters is the same by Lemma 6.7 below. Moreover, the same condition on t ensures that the valuation of the leading term c and of Δ/c remain unchanged (cf. Definition 6.1, Lemma 6.8(i) below).

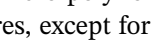
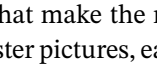
Recall that (for C) $\ell_3 = \alpha_2 + \beta_2$. Now

$$M_t(\alpha_2) + M_t(\beta_2) = \frac{t^2\alpha_1^2(\alpha_2 + \beta_2) + 2t(\alpha_1^2 + \alpha_2\beta_2) + (\alpha_2 + \beta_2)}{(t\alpha_2 + 1)(t\beta_2 + 1)}.$$

Observe that the numerator is the zero polynomial in $k(t)$ if and only if $\alpha_2 \equiv -\beta_2$ and $\alpha_2^2 \equiv \alpha_1^2$ in k. This is equivalent to $\alpha_2 \equiv \pm\alpha_1$ and $\beta_2 \equiv \mp\alpha_1$, which would mean that there is a cluster of depth > 0 containing α_2 and $\pm\alpha_1$ and one containing β_2 and $\mp\alpha_1$. This is not the case for the listed cluster pictures, except for  , so the numerator is not the zero polynomial in $k(t)$ for these. It follows that, so long as t avoids the roots of the polynomial in k and the residues of $-1/\alpha_2, -1/\beta_2$, the expression $M_t(\alpha_2) + M_t(\beta_2)$ will have valuation 0 in $\bar{K}$. Repeating a similar argument for ℓ_2 shows that C_t has $v(\ell_2) = v(\ell_3) = 0$ so long as t avoids a specific list of residue classes of k. For the exceptional cluster picture  , the coefficients of the numerator all have valuation $\geqslant j$, and one similarly checks that at least one has valuation exactly j, so that a suitable choice of t makes $v(\ell_2) = v(\ell_3) = j$.

The arguments for ℓ_1 and η_2, η_3 are similar. Recall that (for C), $\ell_1 = \alpha_2 + \beta_2 - \alpha_3 - \beta_3$. Writing $\mathbf{a} = \alpha_2+\beta_2-\alpha_3-\beta_3$, $\mathbf{b} = \alpha_2\beta_2-\alpha_3\beta_3$ and $\mathbf{c} = \alpha_2\beta_2\alpha_3-\alpha_2\alpha_3\beta_3+\alpha_2\beta_2\beta_3-\alpha_3\beta_2\beta_3$, one checks that

$$\ell_1(C_t) = \frac{\mathbf{a} + 2\mathbf{b}t + (-\alpha_1^2\mathbf{a}+\mathbf{c})t^2 - 2\alpha_1^2\mathbf{b}t^3 - \alpha_1^2\mathbf{c}t^4}{(t\alpha_2+1)(t\beta_2+1)(t\alpha_3+1)(t\beta_3+1)},$$

and that if the numerator reduces to the zero polynomial in $k(t)$, then $\{\bar{\alpha}_2, \bar{\beta}_2\} = \{\bar{\alpha}_3, \bar{\beta}_3\}$. This is not the case in the listed cluster pictures, except for  and  , and picking t that avoids the residue classes that make the numerator or denominator 0 in k makes $v(\ell_1(C_t)) = 0$. For the two exceptional cluster pictures, each coefficient has valuation $\geqslant \min(n, m)$

(respectively, $\geqslant j$), and one easily checks that either $\mathbf{a}$ or $\mathbf{b}$ must have precisely this valuation. Picking t similarly gives $v(\ell_1(C_t)) = \min(n, m)$ (respectively, $= j$).

For η_2, one finds that

$$\eta_2(C_t) = \frac{(\alpha_2^2+\beta_2^2-2\alpha_1^2) + 2t\mathbf{b} + 2t^2\mathbf{c} - 2t^3\alpha_1^2\mathbf{b} + t^4\alpha_1^2(\alpha_1^2\alpha_2^2+\alpha_1^2\beta_2^2-2\alpha_2^2\beta_2^2)}{(t\alpha_2+1)^2(t\beta_2+1)^2},$$

where $\mathbf{b} = (\alpha_2\beta_2-\alpha_1^2)(\alpha_2+\beta_2)$ and $\mathbf{c} = (\alpha_1^2-\alpha_2^2)(\alpha_1^2-\beta_2^2)$. Here the numerator reduces to zero in $k(t)$ only if $\alpha_1^2 \equiv \alpha_2^2 \equiv \beta_2^2$ in k, equivalently only if $\alpha_2 \equiv \pm\alpha_1$ and $\beta_2 \equiv \pm\alpha_1$ (and similarly for η_3). This only happens for  and  of the listed cluster pictures, which make no claim for η_2, η_3. Thus, C_t will have $v(\eta_2) = v(\eta_3) = 0$, so long as t avoids the residue classes that make either the numerators or denominators of $\eta_2(C_t), \eta_3(C_t)$ reduce to 0 in k.

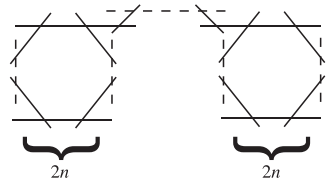
The total number of residue classes t has to avoid is at most 6 (of the form $-1/r$ for a root r, that account for all the denominators) plus 2 + 2 (for ℓ_2, ℓ_3) plus 4 (for ℓ_1) plus 4 + 4 (for η_2, η_3), that is, 22. □

Lemma 6.7. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p and $m = \left(\begin{smallmatrix}\mathbf{a} & \mathbf{b}\\ \mathbf{c} & \mathbf{d}\end{smallmatrix}\right) \in \mathrm{GL}_2(K)$. Suppose that C and C_m are semistable, balanced C2D4 curves over K, and that $r \mapsto m(r)$ induces a bijection between the sets of twins and preserves their relative depths. Then $r \mapsto m(r)$ also commutes with the Galois action on twins and preserves the signs of clusters of even size (after possibly suitably choosing signs of $\theta_{m(\mathfrak{s})}$ for twins $\mathfrak{s}$ of C).*

Proof. Since $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in K$, the Galois action on the roots for C is the same as on the roots on C_m, and so, the map respects the Galois action on twins. It remains to check that it respects signs.

Suppose that C has exactly one twin, $\mathfrak{s}_1$. As the two curves are isomorphic, Theorem 2.17 tells us that the sign must be the same for $\mathfrak{s}_1$ and $m(\mathfrak{s}_1)$ (see types I_n^ϵ and $1 \times \mathrm{I}_n^\epsilon$).

Suppose that C has two twins, $\mathfrak{s}_1$ and $\mathfrak{s}_2$. If these are swapped by Frobenius, then choosing the signs of $\theta_{m(\mathfrak{s}_i)}$ appropriately guarantees that the sign of $\mathfrak{s}_1$ agrees with that of $m(\mathfrak{s}_1)$; by Theorem 2.17, the signs of $\mathfrak{s}_2$ and $m(\mathfrak{s}_2)$ must then also agree (see types $\mathrm{I}_{n\sim n}^\epsilon$ and $\mathrm{I}_n^\epsilon \tilde{\times} \mathrm{I}_n$). If the twins are not swapped but have the same sign, then the result again follows by Theorem 2.17 (types $\mathrm{I}_{n,m}^{+,+}$, $\mathrm{I}_{n,m}^{-,-}$, $\mathrm{I}_n^+ \times \mathrm{I}_m^+$, $\mathrm{I}_n^- \times \mathrm{I}_m^-$). If the twins are not swapped and have different signs and different relative depths, the result follows from the structure of the Néron component group by Remark 2.18, after possibly passing to a quadratic ramified extension (types $\mathrm{I}_{n,m}^{+,-}$, $\mathrm{I}_n^+ \times \mathrm{I}_m^-$ with $n \neq m$). If the twins are not swapped by Frobenius and have different signs (say, + for $\mathfrak{s}_1$ and − for $\mathfrak{s}_2$) and equal relative depths (say $\delta_{\mathfrak{s}_i} = n$), we unfortunately need to use the explicit description of the minimal regular models and the reduction map to the special fibre (see [15, Thm. 8.5 and §5.6]): passing to a quadratic ramified extension if necessary so that n is even, the special fibre of the minimal regular model of C is



and Frobenius fixes the components on the left $2n$-gon and acts as a reflection on the right $2n$-gon. The two Weierstrass points of C that correspond to the roots in the twin $\mathfrak{s}_1$ reduce to the component in the left $2n$-gon that is furthest away from the central chain, corresponding to the fact that the sign of $\mathfrak{s}_1$ is $+$, and the two Weierstrass points for $\mathfrak{s}_2$ reduce to the corresponding component in the right $2n$-gon. As this description is model-independent, it follows that the Möbius transformation must preserve signs of the twins.

Finally, when C and C_m have three twins each, the only signs are those of the full sets of roots. These agree by Theorem 2.17 (types $\mathrm{U}^{\epsilon}_{*}$). □

6.3 | Change of invariants

Lemma 6.8. *Let C be a C2D4 curve over a field K of characteristic 0.*

(i) *For $t \in K \setminus \{\frac{1}{\alpha_1}, -\frac{1}{\alpha_1}\}$,*

$$\Delta(C_t)/c(C_t) = \frac{(1+\alpha_1 t)^2(1-\alpha_1 t)^2}{(1+\alpha_2 t)(1+\beta_2 t)(1+\alpha_3 t)(1+\beta_3 t)} \cdot \Delta(C)/c(C).$$

(ii) *For $m(z) = 1/z$,*

$$\Delta(C_m)/c(C_m) = \frac{1}{\alpha_1^2\alpha_2\beta_2\alpha_3\beta_3} \cdot \Delta(C)/c(C).$$

(ii) *For $m(z) = \lambda z$,*

$$\Delta(C_m)/c(C_m) = \lambda^3 \cdot \Delta(C)/c(C).$$

Proof. Direct computation. □

Lemma 6.9. *Let $K/\mathbb{Q}_p$ be a finite extension with p an odd prime, and let C/K be a C2D4 curve with cluster picture*  *Then*

$$v\left(\frac{\Delta(C)}{c(C)}\right) = 2n + v\left(\frac{\Delta(C_m)}{c(C_m)}\right),$$

for any $m \in \mathrm{GL}_2(K)$ such that C_m/K is balanced.

Proof. Enlarging K if necessary, we may pick $z \in K$ which has $v(z-r) = n$ for the roots inside the cluster of size 5 of C and $v(z-r) = 0$ for the remaining root. One checks that applying the following Möbius transformation yields a model C_m with a balanced cluster picture: $m : x \mapsto x - z \mapsto \frac{1}{x-z} \mapsto \frac{\pi_K^n}{x-z}$. By Lemma 6.8, $v(\Delta(C_m)) - v(c(C_m)) = v(\Delta) - v(c) - 5n + 3n$.

It remains to show that if C and C_m are both balanced models, then $v(\Delta(C)) = v(\Delta(C_m))$. As Δ is invariant under shifts of the x-coordinate, we may assume that both C and C_m are centred; in particular, $\alpha_1(C)$ and $\alpha_1(C_m)$ are both units. By Lemma 6.4, the associate

Möbius transformation is of the form $m = r \circ M_t$ for some t, where $r(z) = \lambda z$ and $\lambda = \frac{\alpha_1(C_m)}{\alpha_1(C)} \in K^{nr}$. As the roots are integral with distinct images in the residue field for both curves, we find that $t \not\equiv \pm\alpha_1^{-1}, \alpha_2^{-1}, -\beta_2^{-1}, \alpha_3^{-1}, -\beta_3^{-1}$ in the residue field. The result now follows from Lemma 6.8(i). □

Lemma 6.10. *For a C2D4 curve C over a field K of characteristic 0 and $m \in \mathrm{GL}_2(K)$,*

$$\hat\delta_1(C) = \hat\delta_1(C_m) \cdot \square.$$

Proof. As $\hat\delta_1$ is invariant under shifts of the x-coordinate, we may assume that both C and C_m are centred. By Lemma 6.4, the associate Möbius transformation is of the form $m = r \circ M_t$ for some $t \in K \cup \{\infty\}$, where $r(z) = \lambda z$ and $\lambda = \frac{\alpha_1(C_m)}{\alpha_1(C)} \in K$. As $c^2\hat\delta_1$ is a homogeneous rational function of even degree in the roots, $\hat\delta_1(C_t) = \hat\delta_1(C_m) \cdot \square$. As $\hat\delta_1 = (\frac{\ell_1}{2\Delta})^2(\hat\alpha_1 - \hat\beta_1)^2$ (see Definition 2.1) and $\ell_1/\Delta \in K$, it suffices to check that $(\hat\alpha_1(C) - \hat\beta_1(C))^2 = (\hat\alpha_1(C_t) - \hat\beta_1(C_t))^2 \cdot \square$. Explicit computation shows that

$$\begin{aligned}&(\hat\alpha_1(C_t) - \hat\beta_1(C_t))^2\\ &\quad= (\hat\alpha_1(C) - \hat\beta_1(C))^2 \frac{(-1+\alpha_1^2t^2)^2 \cdot (\alpha_2 - \alpha_3 + \beta_2 - \beta_3)^2}{(\ell_1(C) + (2\alpha_2\beta_2 - 2\alpha_3\beta_3)t + (\alpha_2\alpha_3\beta_2 - \alpha_2\alpha_3\beta_3 + \alpha_2\beta_2\beta_3 - \alpha_3\beta_2\beta_3)t^2)^2},\end{aligned}$$

with the natural extension of the formula to $t = \infty$. □

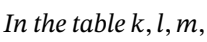
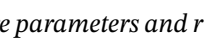
7 | ODD PLACES

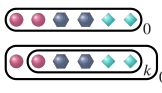
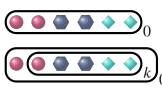
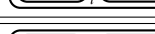
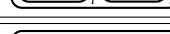
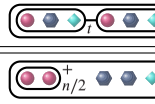
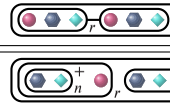
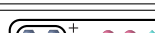
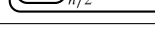
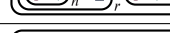
Here, we state an analogue of Theorem 5.2 for C2D4 curves over finite extensions of $\mathbb{Q}_p$ for odd primes p. Its proof will occupy §8 and §9. We will remove the constraints on valuations in Theorem 12.2 and extend it to all semistable curves in Theorem 12.5.

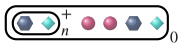
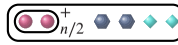
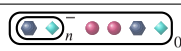
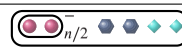
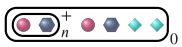
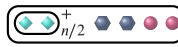
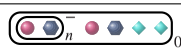
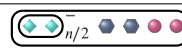
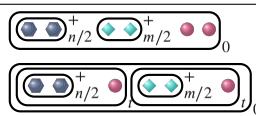
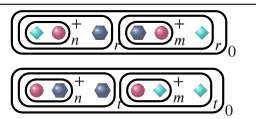
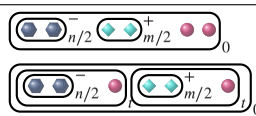
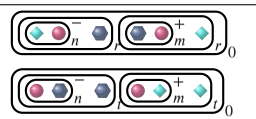
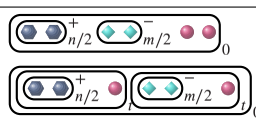
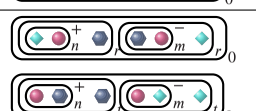
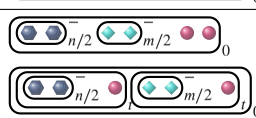
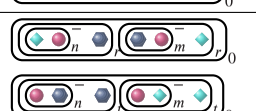
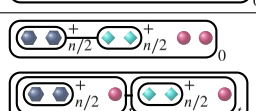
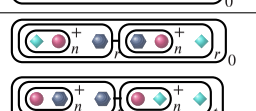
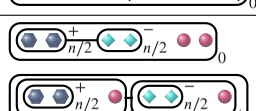
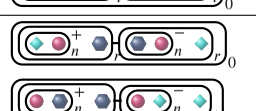
Theorem 7.1. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\ell_1, \ell_2, \ell_3, \Delta \neq 0$ whose cluster picture with Frobenius action is one of the cases described in the table below. Let J and $\widehat J$ be the Jacobians of C and $\widehat C$.*

Then $c_{J/K}$, $\mu_{C/K}$, $c_{\widehat J/K}$, $\mu_{\widehat C/K}$, $\lambda_{C/K}$ and $w_{C/K}$ are given by the corresponding columns in the table. If the residue field has size $|k| \geqslant 23$, then $\widehat C$ admits a model whose cluster picture with Frobenius action is given in the $\widehat C$ column. $E_{C/K}$ is as given in the table provided $\mathcal{P}, \eta_1 \neq 0$ and:

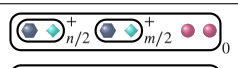
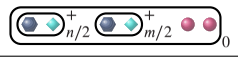
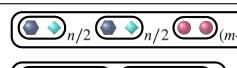
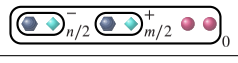
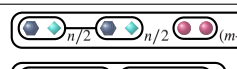
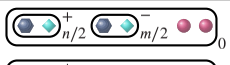
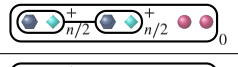
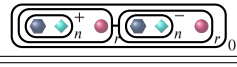
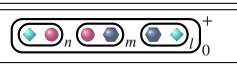
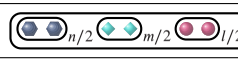
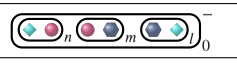
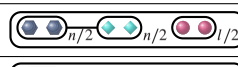
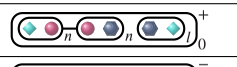
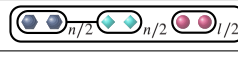
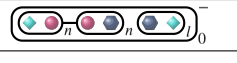
- $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ *in cases* $1_n^\epsilon(a,b)$, $1_{2n}^\epsilon(c,d)$ *and* $1 \times_t \mathrm{I}_n^\epsilon(a)$,
- $v(\ell_1) = v(\ell_2) = v(\ell_3) = 0$ *in cases* $\mathrm{I}_{n,m}^{\epsilon,\delta}(a)$, $\mathrm{I}_{n\sim n}^{\epsilon}(a)$,
- $v(\ell_1) = t$ *in cases* $1\times_t 1(b,c)$ *and* $1\tilde\times_t 1(b,c)$ *and*
- $v(\ell_1) = \frac{n}{2}$, $v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ *in cases* $\mathrm{I}_{n,m}^{\epsilon,\delta}(b)$ *and* $\mathrm{I}_{n\sim n}^{\epsilon}(b)$.

In the table $k, l, m, n, t \in \mathbb{Z}_{>0}$ are parameters and $r \in \mathbb{Z}$ is defined by the column of $v(\Delta/c)$. In the $\widehat C$ column, a cluster of size 3 with index 0 means that the roots in it do not form a cluster, for example,  *with $r = 0$ means*  .

Case	C	$v(\Delta/c)$	$\widehat{C}$	$c_{J/K}$	$\mu_{C/K}$	$c_{\widehat{J}/K}$	$\mu_{\widehat{C}/K}$	$\lambda_{C/K}$	$w_{C/K}$	$E_{C/K}$
$2(a)$ $2(b)$ $2(c)$	 $\hat{\delta}_1 \in K^{\times 2}$	r $2k+r$ $2k+r$		1	1	1	1	1	1	1
$2(d)$ $2(e)$ $2(f)$	 $\hat{\delta}_1 \notin K^{\times 2}$	r $2k+r$ $2k+r$		1	1	1	$(-1)^r$	$(-1)^r$	1	$(-1)^r$
$1\times_t 1(a)$				1	1	1	1	1	1	1
$1\tilde{\times}_t 1(a)$				1	$(-1)^t$	1	$(-1)^t$	1	1	1
$1\times_t 1(b)$	 $\hat{\delta}_1 \in K^{\times 2}$	$2t+r$		1	1	1	1	1	1	1
$1\times_t 1(c)$	 $\hat{\delta}_1 \notin K^{\times 2}$	$2t+r$		1	1	1	$(-1)^r$	$(-1)^r$	1	$(-1)^r$
$1\tilde{\times}_t 1(b)$	 $\hat{\delta}_1 \in K^{\times 2}$	$2t+r$		1	$(-1)^t$	1	1	$(-1)^t$	1	$(-1)^t$
$1\tilde{\times}_t 1(c)$	 $\hat{\delta}_1 \notin K^{\times 2}$	$2t+r$		1	$(-1)^t$	1	$(-1)^r$	$(-1)^{t+r}$	1	$(-1)^{t+r}$
$1_n^+(a)$ $1\times_t \mathrm{I}_n^+(a)$		r		n	1	$2n$	1	-1	-1	1
$1_n^-(a)$ $1\times_t \mathrm{I}_n^-(a)$		r		$\widetilde{n}$	1	2	1	$(-1)^n$	1	$(-1)^n$
$1_n^+(b)$		r		n	1	$2n$	1	-1	-1	1
$1_n^-(b)$		r		$\widetilde{n}$	1	2	1	$(-1)^n$	1	$(-1)^n$

Case	C	$v(\Delta/c)$	$\widehat{C}$	$c_{J/K}$	$\mu_{C/K}$	$c_{\hat{J}/K}$	$\mu_{\widehat{C}/K}$	$\lambda_{C/K}$	$w_{C/K}$	$E_{C/K}$
$1^{+}_{2n}(c)$				$2n$	1	n	1	-1	-1	1
$1^{-}_{2n}(c)$				2	1	$\widetilde{n}$	1	$(-1)^n$	1	$(-1)^n$
$1^{+}_{2n}(d)$				$2n$	1	n	1	-1	-1	1
$1^{-}_{2n}(d)$				2	1	$\widetilde{n}$	1	$(-1)^n$	1	$(-1)^n$
$\mathrm{I}^{+,+}_{n,m}(a)$ $\mathrm{I}^{+}_{n}\times_t \mathrm{I}^{+}_{m}(a)$		r		nm	1	$4nm$	1	1	1	1
$\mathrm{I}^{-,+}_{n,m}(a)$ $\mathrm{I}^{-}_{n}\times_t \mathrm{I}^{+}_{m}(a)$		r		$\widetilde{n}m$	1	$4m$	1	$(-1)^{n+1}$	-1	$(-1)^n$
$\mathrm{I}^{+,-}_{n,m}(a)$ $\mathrm{I}^{+}_{n}\times_t \mathrm{I}^{-}_{m}(a)$		r		$n\widetilde{m}$	1	$4n$	1	$(-1)^{m+1}$	-1	$(-1)^m$
$\mathrm{I}^{-,-}_{n,m}(a)$ $\mathrm{I}^{-}_{n}\times_t \mathrm{I}^{-}_{m}(a)$		r		$\widetilde{n}\widetilde{m}$	1	4	1	$(-1)^{n+m}$	1	$(-1)^{n+m}$
$\mathrm{I}^{+}_{n\sim n}(a)$ $\mathrm{I}^{+}_{n}\widetilde{\times}_t \mathrm{I}_{n}(a)$		r		n	1 $(-1)^t$	$2n$	$(-1)^r$ $(-1)^t$	$(-1)^{r+1}$ -1	-1	$(-1)^r$ 1
$\mathrm{I}^{-}_{n\sim n}(a)$ $\mathrm{I}^{-}_{n}\widetilde{\times}_t \mathrm{I}_{n}(a)$		r		$\widetilde{n}$	1 $(-1)^t$	2	$(-1)^r$ $(-1)^t$	$(-1)^{n+r}$ $(-1)^n$	1	$(-1)^{n+r}$ $(-1)^n$

Notation: $\tilde{x} = 2$ if $2|x$ and $\tilde{x} = 1$ if $2 \nmid x$.

Case	C	$v(\Delta/c)$	$\widehat{C}$	$c_{J/K}$	$\mu_{C/K}$	$c_{\hat{J}/K}$	$\mu_{\widehat{C}/K}$	$\lambda_{C/K}$	$w_{C/K}$	$E_{C/K}$
$\mathrm{I}^{+,+}_{n,m}(b)$	 $n<m$  $n=m$	$\frac{n}{2}+r$		nm	1	$4nm$	1	1	1	1
$\mathrm{I}^{-,+}_{n,m}(b)$	 $n<m$  $n=m$	$\frac{n}{2}+r$		$\widetilde{n}m$	1	m	$(-1)^{r}$	$(-1)^{n+1+r}$	-1	$(-1)^{n+r}$
$\mathrm{I}^{+,-}_{n,m}(b)$	 $n<m$  $n=m$	$\frac{n}{2}+r$		$n\widetilde{m}$	1	n	$(-1)^{\frac{m-n}{2}+r}$	$(-1)^{\frac{m+n}{2}+r+1}$	-1	$(-1)^{\frac{n+m}{2}+r}$
$\mathrm{I}^{-,-}_{n,m}(b)$	 $n<m$  $n=m$	$\frac{n}{2}+r$		$\widetilde{n}\widetilde{m}$	1	$(\widetilde{\frac{nm}{D}})\widetilde{D}$	$(-1)^{n\frac{m-n}{2}}$	$(-1)^{\frac{m-n}{2}}$	1	$(-1)^{\frac{m-n}{2}}$
$\mathrm{I}^{+}_{n\sim n}(b)$		$\frac{n}{2}+r$		n	1	$n\widetilde{n}$	1	$(-1)^{n+1}$	-1	$(-1)^{n}$
$\mathrm{I}^{-}_{n\sim n}(b)$		$\frac{n}{2}+r$		$\widetilde{n}$	1	$\widetilde{n}$	$(-1)^{r}$	$(-1)^{r}$	1	$(-1)^{r}$
$\mathrm{U}^{+}_{n,m,l}(a)$				N	1	$4N$	1	1	1	1
$\mathrm{U}^{-}_{n,m,l}(a)$				$(\widetilde{\frac{N}{M}})\widetilde{M}$	$(-1)^{nml}$	4	1	$(-1)^{n+m+l}$	1	$(-1)^{n+m+l}$
$\mathrm{U}^{+}_{n\sim n,l}(a)$				$n+2l$	1	$2n+4l$	1	-1	-1	1
$\mathrm{U}^{-}_{n\sim n,l}(a)$				n	$(-1)^{l}$	$2n$	1	$(-1)^{l+1}$	-1	$(-1)^{l}$

Notation: $\tilde{x}=2$ if $2|x$ and $\tilde{x}=1$ if $2\nmid x$, $D=gcd(n,\frac{m-n}{2})$, $N=nm+nl+ml$, $M=gcd(n,m,l)$.

Remark 7.2. In the cases $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$, the semistability criterion (Theorem 2.12) and the C2D4 structure on C ensure that $n \equiv m \bmod 2$. Indeed, n is odd if and only if inertia permutes the roots in the corresponding twin. The C2D4 structure then forces inertia to permute the roots in the twin of depth $m/2$.

8 | ODD PLACES: CHANGE OF INVARIANTS UNDER ISOGENY

In this section, we prove the claim of Theorem 7.1 regarding Tamagawa numbers and deficiency and the cluster picture of $\widehat{C}$ when K has odd residue characteristic.

Theorem 8.1. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p. Let C/K be a semistable C2D4 curve with $\ell_1, \ell_2, \ell_3, \Delta \neq 0$ whose cluster picture with Frobenius action is one of the cases in the table of Theorem 7.1. Let J and $\widehat{J}$ be the Jacobians of C and $\widehat{C}$. Then*

(1) *$c_{J/K}$, $\mu_{C/K}$, $c_{\widehat{J}/K}$, $\mu_{\widehat{C}/K}$, $\lambda_{C/K}$ and $w_{C/K}$ are as given in the table.*
(2) *If the residue field has size $|k| \geqslant 23$, then $\widehat{C}$ admits a model whose cluster picture with Frobenius action is given in the $\widehat{C}$ column of the table.*

Proof.

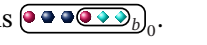
(2) $\Rightarrow$ (1). The formulae for $c_{J/K}, \mu_{C/K}$ and $w_{C/K}$ follow directly from Theorem 2.17. To determine $c_{\widehat{J}/K}$ and $\mu_{\widehat{J}/K}$, we may first pass to an unramified extension of sufficiently large degree so that $|k| \geqslant 23$ (Lemma 3.7). As these invariants are independent of the choice of model, we can change the model of $\widehat{C}$ using (2) to one with the specified cluster picture; the values for $c_{\widehat{J}/K}$ and $\mu_{\widehat{C}/K}$ then follow from Theorem 2.17. By Lemma 3.4, $\lambda_{J/K} = \mu_{C/K}\mu_{\widehat{C}/K}(-1)^{\mathrm{ord}_2(c_{J/K}/c_{\widehat{J}/K})}$, which gives the required values for λ.

(2) First, note that if C' is a different model for C obtained by a Möbius transformation on the x-coordinate (as in Definition 6.1), there is an isomorphism between $\mathrm{Jac}\,\widehat{C}$ and $\mathrm{Jac}\,\widehat{C}'$ that preserves the kernel of the corresponding isogeny. So, $\mathrm{Jac}\,\widehat{C}$ and $\mathrm{Jac}\,\widehat{C}'$ are isomorphic as abelian varieties with a principal polarisation, and hence, $\widehat{C}'$ is isomorphic to $\widehat{C}$ by Torelli's theorem (see [25, Cor. 12.2]). We may therefore change the model of C to ensure that it is centred and balanced (Theorem 6.5) and that it satisfies the conclusions of Theorem 6.6. This change of model does not change whether $\hat{\delta}_1 \in K^{\times 2}$ (Lemma 6.10) or the definition of r (Lemma 6.9 for cases 2(a–f)). In particular, cases 2(b,c,e,f) will follow from cases 2(a,d). Note also that the cluster picture of $\widehat{C}$ depends on the choice of Richelot isogeny on C, but not on the particular choice of C2D4 structure, so that cases 1^{ϵ}_{n}(b,d) will follow from cases 1^{ϵ}_{n}(a,c).

By changing the model, it will thus suffice to establish the result for the following list of cases with the given simplifying hypotheses granted by Theorem 6.6; here $\epsilon, \delta = \pm$ are independent signs. These are proved in the sections indicated:

- 2(a,d), $1\times_t 1$(a) and $1\tilde{\times}_t 1$(a) with $v(\ell_i) = 0$ for $i = 1, 2, 3$, (§8.2),
- $1\times_t 1$(b,c) and $1\tilde{\times}_t 1$(b,c) with $v(\ell_i) = t$ for $i = 1, 2, 3$, (§8.2),
- 1^{ϵ}_{n}(a,c) and $1\times_t \mathrm{I}^{\epsilon}_{n}$(a) with $v(\ell_i) = 0$ for $i = 1, 2, 3$, (§8.3),
- $\mathrm{I}^{\epsilon,\delta}_{n,m}$(a), $\mathrm{I}^{\epsilon}_{n\sim n}$(a), $\mathrm{I}^{\epsilon}_{n}\times_t \mathrm{I}^{\delta}_{m}$(a), $\mathrm{I}^{\epsilon}_{n}\tilde{\times}_t \mathrm{I}_{n}$(a), $\mathrm{U}^{\epsilon}_{n,m,l}$(a), $\mathrm{U}^{\epsilon}_{n\sim n,l}$(a) with $v(\ell_i) = 0$ for $i = 1, 2, 3$, (§8.4),
- $\mathrm{I}^{\epsilon,\delta}_{n,m}$(b) and $\mathrm{I}^{\epsilon}_{n\sim n}$(b) with $v(\ell_1) = \frac{n}{2}$, $v(\ell_2) = v(\ell_3) = 0$ (§8.4). □

We will use without further mention that in all of the above cases, the roots of C and of $\widehat{C}$ are integral, that is, $v(\alpha_i), v(\beta_i), v(\hat{\alpha}_i), v(\hat{\beta}_i) \geqslant 0$. This follows from Lemma 2.11 and, in cases $1\times_t 1$(b,c), $1\tilde{\times}_t 1$(b,c), $\mathrm{I}^{\epsilon,\delta}_{n,m}$(b) and $\mathrm{I}^{\epsilon}_{n\sim n}$(b), from the explicit formula in Lemma 8.3 below.

Notation 8.2. Throughout this section, for drawing cluster pictures, we will use the convention as in Theorem 7.1, that a cluster (other than $\mathcal{R}$) with an index 0 means that the roots in it do not form a cluster. For example, when $a = 0$, the cluster picture  means  .

8.1 | Preliminary results

To control the cluster picture of $\widehat{C}$, we will extensively use the following observations.

Lemma 8.3. *For a C2D4 curve with $\ell_1, \ell_2, \ell_3 \neq 0$, the roots of the Richelot dual curve are*

$$\hat{\alpha}_1, \hat{\beta}_1 = \frac{1}{\ell_1}\left(\alpha_2\beta_2 - \alpha_3\beta_3 \pm \sqrt{(\alpha_2-\alpha_3)(\alpha_2-\beta_3)(\beta_2-\alpha_3)(\beta_2-\beta_3)}\right),$$
$$\hat{\alpha}_2, \hat{\beta}_2 = \frac{1}{\ell_2}\left(\alpha_3\beta_3 - \alpha_1\beta_1 \pm \sqrt{(\alpha_3-\alpha_1)(\alpha_3-\beta_1)(\beta_3-\alpha_1)(\beta_3-\beta_1)}\right),$$
$$\hat{\alpha}_3, \hat{\beta}_3 = \frac{1}{\ell_3}\left(\alpha_2\beta_2 - \alpha_1\beta_1 \pm \sqrt{(\alpha_2-\alpha_1)(\alpha_2-\beta_1)(\beta_2-\alpha_1)(\beta_2-\beta_1)}\right).$$

Proof. This follows by solving the defining quadratic polynomials $\hat{r}(x), \hat{s}(x), \hat{t}(x)$. □

Proposition 8.4. *For a C2D4 curve C with $\Delta, \ell_1, \ell_2, \ell_3 \neq 0$,*

(1) $\ell_1^2\,(\hat{\alpha}_1-\hat{\beta}_1)^2 = \;\; 4\,(\alpha_2-\alpha_3)(\alpha_2-\beta_3)(\beta_2-\alpha_3)(\beta_2-\beta_3)$,
(2) $\ell_2^2\,(\hat{\alpha}_2-\hat{\beta}_2)^2 = \;\; 4\,(\alpha_3-\alpha_1)(\alpha_3-\beta_1)(\beta_3-\alpha_1)(\beta_3-\beta_1)$,
(3) $\ell_3^2\,(\hat{\alpha}_3-\hat{\beta}_3)^2 = \;\; 4\,(\alpha_2-\alpha_1)(\alpha_2-\beta_1)(\beta_2-\alpha_1)(\beta_2-\beta_1)$,
(4) $(\alpha_1-\beta_1)^2 = \frac{c^2\ell_2^2\ell_3^2}{\Delta^2}(\hat{\alpha}_2-\hat{\alpha}_3)(\hat{\alpha}_2-\hat{\beta}_3)(\hat{\beta}_2-\hat{\alpha}_3)(\hat{\beta}_2-\hat{\beta}_3)$,
(5) $(\alpha_2-\beta_2)^2 = \frac{c^2\ell_1^2\ell_3^2}{\Delta^2}(\hat{\alpha}_3-\hat{\alpha}_1)(\hat{\alpha}_3-\hat{\beta}_1)(\hat{\beta}_3-\hat{\alpha}_1)(\hat{\beta}_3-\hat{\beta}_1)$,
(6) $(\alpha_3-\beta_3)^2 = \frac{c^2\ell_1^2\ell_2^2}{\Delta^2}(\hat{\alpha}_1-\hat{\alpha}_2)(\hat{\alpha}_1-\hat{\beta}_2)(\hat{\beta}_1-\hat{\alpha}_2)(\hat{\beta}_1-\hat{\beta}_2)$,
(7) $\Delta(\widehat{C}) = \frac{2}{c^2}\Delta(C)$.

Proof. These are purely algebraic identities that can be verified using Lemma 8.3. □

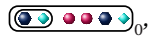
Lemma 8.5. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p. Suppose that C and C' are semistable curves of genus 2 over K, whose Jacobians are isogenous. Then both curves are in the same list of types given below (in the sense of Theorem 2.17, possibly with different parameters):*

(1) *Types* 2, 1×1, $1\tilde{\times}1$;
(2) *Types* 1^+_n, $1\times \mathrm{I}^+_n$;
(3) *Types* 1^-_n, $1\times \mathrm{I}^-_n$;
(4) *Types* $\mathrm{I}^{+,+}_{n,m}$, $\mathrm{U}^+_{n,m,k}$, $\mathrm{I}^+_n\times\mathrm{I}^+_m$;

(5) *Types* $\mathrm{I}^{+,-}_{n,m}$, $\mathrm{I}^{-,+}_{n,m}$, $\mathrm{I}^{+}_{n\sim n}$, $\mathrm{U}^{+}_{n\sim n,k}$, $\mathrm{U}^{-}_{n\sim n,k}$, $\mathrm{I}^{+}_{n}\times\mathrm{I}^{-}_{m}$, $\mathrm{I}^{-}_{n}\times\mathrm{I}^{+}_{m}$, $\mathrm{I}^{+}\tilde{\times}\mathrm{I}_{n}$;
(6) *Types* $\mathrm{I}^{-,-}_{n,m}$, $\mathrm{U}^{-}_{n,m,k}$, $\mathrm{I}^{-}_{n}\times\mathrm{I}^{-}_{m}$;
(7) *Type* $\mathrm{U}^{+}_{n\sim n\sim n}$;
(8) *Type* $\mathrm{U}^{-}_{n\sim n\sim n}$;
(9) *Types* $\mathrm{I}^{-}_{n\sim n}$, $\mathrm{I}^{-}_{n}\tilde{\times}\mathrm{I}_{n}$.

Proof. Since the isogeny induces an isomorphism on Galois representations, the eigenvalues of Frobenius on the toric part of the Galois representation (equivalently, on the homology of the dual graph of the special fibre of the minimal regular model) for the two curves must be the same. By [15, Thm. 18.8], the nine lists given correspond to eigenvalues (with multiplicity) being $\emptyset, \{1\}, \{-1\}, \{1,1\}, \{1,-1\}, \{-1,-1\}, \{\zeta_3, \zeta_3^{-1}\}, \{\zeta_6, \zeta_6^{-1}\}, \{\zeta_4, \zeta_4^{-1}\}$, where ζ_n denotes a primitive nth root of unity. □

Lemma 8.6. *Let $K/\mathbb{Q}_p$ be a finite extension and C/K a C2D4 curve with $v(\alpha_i), v(\beta_i) \geqslant 0$.*

(1) *If the cluster picture of C is either*  ,  ,  ,  ,  ,  *or*  , *then $v(\Delta/c) = 0$.*
(2) *If p is odd and the cluster picture of C is*  , *then $v(\Delta/c) = 0$.*
(3) *If C has a cluster of positive depth d that contains a root of each colour, then $v(\Delta/c) \geqslant d$.*

Proof.

(1, 3) Suppose that there is a cluster of depth d that contains two roots of different colour: without loss of generality α_2 and α_3. Then substituting $\alpha_2 \equiv \alpha_3 \bmod \pi_K^d$ into the expression for Δ gives $\Delta/c \equiv (\beta_2-\beta_3)(\alpha_1-\alpha_2)(\beta_1-\alpha_2) \bmod \pi_K^d$. For the pictures in (1), each term is a unit, so Δ/c is a unit. For (3), either α_1 or β_1 is in the same cluster as α_2 and α_3, so the corresponding term is $\equiv 0 \bmod \pi_K^d$, and hence so is Δ/c.
(2) In this case $\Delta/c \equiv 2(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)(\alpha_3-\alpha_2)$ in the residue field, which is a unit. □

Lemma 8.7. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p with residue field of size $|k| > 3$. Let C/K be a semistable C2D4 curve whose cluster picture has two clusters $\mathfrak{s}, \mathfrak{s}'$ of size 3 with relative depth $\delta_{\mathfrak{s}} = 2r - z$ and $\delta_{\mathfrak{s}'} = z$ for some integers $0 \leqslant z \leqslant r$; we allow for the case $z = 0$ when $\mathfrak{s}'$ is not a cluster and $\mathfrak{s}$ is a cluster that is not contained in a cluster of size 4 or 5. Then C admits another model with an identical cluster picture except for which $\delta_{\mathfrak{s}} = \delta_{\mathfrak{s}'} = r$ (and all colours, clusters, signs, Frobenius action on proper clusters, other relative depths and the depth of the full set of roots the same as for C).*

Proof. This is essentially [15, Prop. 14.6(4)]. Write $\mathcal{R}$ for the set of roots for C.

If Galois swaps the two clusters, then they necessarily have the same depth, so there is nothing to prove. We may thus assume that $\mathfrak{s}$ is Galois stable.

Pick $z_{\mathfrak{s}} \in K$ such that $v(r - z_{\mathfrak{s}}) \geqslant d_{\mathfrak{s}}$ for $r \in \mathfrak{s}$, and similarly $z_{\mathfrak{s}'}$ for $\mathfrak{s}'$. (This exists by [15, Lemma B.1 and Thm. 2.12], which ensures that $K(\mathcal{R})/K$ is tame; if $p \neq 3$, one may simply take $z_{\mathfrak{s}}$ to be the average of the roots in $\mathfrak{s}$.) Since $z_{\mathfrak{s}}, z_{\mathfrak{s}'} \in K$, it follows that $v(z_{\mathfrak{s}} - z_{\mathfrak{s}'}) \in \mathbb{Z}$ and hence $d_{\mathcal{R}} \in \mathbb{Z}$. Applying a Möbius transformation of the form $x \mapsto \pi_K^n x$, we may assume that $d_{\mathcal{R}} = 0$. Applying a further Möbius transformation of the form $x \mapsto x - z_{\mathfrak{s}} + u\pi_K^{r-z}$ for a suitable unit u, we may assume that $v(r) = r - z$ for roots $r \in \mathfrak{s}$ and $v(r) = 0$ for $r \in \mathfrak{s}'$.

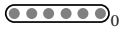
Now observe that for roots r, r',

$$v\left(\frac{\pi_K^n}{r}-\frac{\pi_K^n}{r'}\right)=v(r-r')+n-v(r)-v(r').$$

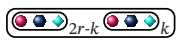
Thus, applying the Möbius transformation $x\mapsto\frac{\pi_K^{r-z}}{x}$ now gives a model for C with the desired cluster picture. The colouring and Frobenius action on proper clusters are clearly preserved. The signs of twins (these are the only clusters with signs here) are preserved by Lemma 6.7. □

8.2 | Proof of Theorem 8.1: Toric dimension 0

Consider cases 2(a,d), 1×1(a,b,c) and 1$\tilde{\times}$1(a,b,c). By Lemma 8.5, $\widehat{C}$ has Type 2, 1×1 or 1$\tilde{\times}$1, and, in particular, its cluster picture has no clusters of size 2 or 4 (Theorem 2.17).

Cases 2(a,d), $1\times_t 1$(b,c) and $1\tilde{\times}_t 1$(b,c). Here $v(\Delta/c)=2t+r$, with $t=0$ for cases 2(a,d). Proposition 8.4(1,2,3) gives $v(\hat{\alpha}_1-\hat{\beta}_1)=v(\hat{\alpha}_2-\hat{\beta}_2)=v(\hat{\alpha}_3-\hat{\beta}_3)=0$, so the cluster picture of $\widehat{C}$ is either  ,  or  . Proposition 8.4(4) gives

$$v((\hat{\alpha}_2-\hat{\alpha}_3)(\hat{\alpha}_2-\hat{\beta}_3)(\hat{\beta}_2-\hat{\alpha}_3)(\hat{\beta}_2-\hat{\beta}_3))=2r,$$

so the cluster picture is  for some $0\leqslant k\leqslant 2r$.

An automorphism $\sigma\in\mathrm{Gal}(\bar{K}/K)$ swaps the two clusters of size 3 if and only if it swaps $\hat{\alpha}_1$ and $\hat{\beta}_1$. Since $\Delta/\ell_1\in K$, Proposition 8.4(1) and the definition of $\hat{\delta}_1$ show that this is equivalent to $\sigma(\sqrt{\hat{\delta}_1})=-\sqrt{\hat{\delta}_1}$. Lemma 8.7 gives the required model for $\widehat{C}$.

Cases $1\times_t 1$(a) and $1\tilde{\times}_t 1$(a). By Lemma 8.6, $v(\Delta/c)=0$. Proposition 8.4(1,4) gives

$$v(\hat{\alpha}_1-\hat{\beta}_1)=0,\qquad v((\hat{\alpha}_2-\hat{\alpha}_3)(\hat{\alpha}_2-\hat{\beta}_3)(\hat{\beta}_2-\hat{\alpha}_3)(\hat{\beta}_2-\hat{\beta}_3))=0,$$

which force the cluster picture of $\widehat{C}$ to be  , for some $a,b\geqslant 0$. Proposition 8.4(2,3) gives $v(\hat{\alpha}_2-\hat{\beta}_2)=v(\hat{\alpha}_3-\hat{\beta}_3)=t$, so that $a=b=t$.

The expression on the right-hand side of Proposition 8.4(1) is K-rational and a perfect square in the residue field. Hence, a Galois element swaps the two clusters of $\widehat{C}$ if and only if it swaps $\hat{\alpha}_1$ and $\hat{\beta}_1$, if and only if it maps ℓ_1 to $-\ell_1$, if and only if it swaps the two clusters of C.

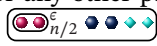
8.3 | Proof of Theorem 8.1: Toric dimension 1

Consider cases 1^{ϵ}_n(a), 1^{ϵ}_{2n}(c) and $1\times_t \mathrm{I}^{\epsilon}_n(a)$. By Lemma 8.5, $\widehat{C}$ will have either type 1^{ϵ}_* or $1\times_* \mathrm{I}^{\epsilon}_*$ for some suitable $*$s. In particular, its cluster picture will have a cluster of size 2 or 4, but will not have two clusters of size 2 (Theorem 2.17).

Case 1^{ϵ}_n(a). Here $r=v(\Delta/c)\geqslant 0$. Proposition 8.4(1,2,3) and the cluster picture of C yield $v(\hat{\alpha}_i-\hat{\beta}_i)^2=0$ for $i=1,2,3$. Hence, the cluster picture of $\widehat{C}$ has no cluster of size $\geqslant 4$, so that it is either  ,  ,  or  . Relabelling $\hat{\alpha}_i\leftrightarrow\hat{\beta}_i$ if necessary, we may assume that $\hat{\alpha}_1,\hat{\alpha}_2,\hat{\alpha}_3$ are the three leftmost roots in these pictures, so that $v(\hat{\alpha}_i-\hat{\beta}_j)=0$ for all i,j. Proposition 8.4(4,5,6) then gives

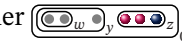
$$v((\hat{\alpha}_2-\hat{\alpha}_3)(\hat{\beta}_2-\hat{\beta}_3))=2r+n,\quad v((\hat{\alpha}_3-\hat{\alpha}_1)(\hat{\beta}_3-\hat{\beta}_1))=v((\hat{\alpha}_1-\hat{\alpha}_2)(\hat{\beta}_1-\hat{\beta}_2))=2r.$$

It follows that the cluster picture of $\widehat{C}$ with Frobenius action is  for some $0 \leqslant z \leqslant 2r$. Lemma 8.7 gives the required model for $\widehat{C}$.

Cases 1^{ϵ}_{2n} (c). By Lemma 8.6, $v(\Delta/c)=0$, so by Proposition 8.4, $v(\hat{\alpha}_1-\hat{\beta}_1)=\frac{n}{2}$, and $v(r_1-r_2)=0$ for any other pair of roots r_1, r_2 for $\widehat{C}$. The cluster picture with Frobenius action of $\widehat{C}$ is therefore  .

Case $1\times_t \mathrm{I}^{\epsilon}_n$ (a). By Lemma 8.6, $v(\Delta/c)=0$. By Propostion 8.4(2,5),

$$v(\hat{\alpha}_2-\hat{\beta}_2)=v((\hat{\alpha}_3-\hat{\alpha}_1)(\hat{\alpha}_3-\hat{\beta}_1)(\hat{\beta}_3-\hat{\alpha}_1)(\hat{\beta}_3-\hat{\beta}_1))=0.$$

Thus, there is no cluster that contains both the sapphire roots, or both a ruby and a turquoise root. In particular, there are no clusters of size 4 or 5 and the cluster picture of $\widehat{C}$ is either  or  for some $w>0$ and $y, z \geqslant 0$. Proposition 8.4 also gives

$$v(\hat{\alpha}_1-\hat{\beta}_1)=v(\hat{\alpha}_3-\hat{\beta}_3)=t,$$

$$v((\hat{\alpha}_2-\hat{\alpha}_3)(\hat{\alpha}_2-\hat{\beta}_3)(\hat{\beta}_2-\hat{\alpha}_3)(\hat{\beta}_2-\hat{\beta}_3))=n+2t,$$

$$v((\hat{\alpha}_1-\hat{\alpha}_2)(\hat{\alpha}_1-\hat{\beta}_2)(\hat{\beta}_1-\hat{\alpha}_2)(\hat{\beta}_1-\hat{\beta}_2))=2t,$$

so the cluster picture with Frobenius action must be  .

8.4 | Proof of Theorem 8.1: Toric dimension 2

Consider cases $\mathrm{I}^{\epsilon,\delta}_{n,m}$(a,b), $\mathrm{I}^{\epsilon}_{n\sim n}$(a,b), $\mathrm{I}^{\epsilon}_n\times\mathrm{I}^{\delta}_m$, $\mathrm{I}^{\epsilon}_n\tilde{\times}\mathrm{I}_n$, $\mathrm{U}^{\epsilon}_{n,m,l}$ and $\mathrm{U}^{\epsilon}_{n\sim n,l}$. By Lemma 8.5, $\widehat{C}$ will have type $\mathrm{I}_{*,*}$, $\mathrm{I}_*\times\mathrm{I}_*$, $\mathrm{I}_*\tilde{\times}\mathrm{I}_*$ or U_{***}, with some subscripts and signs. In particular, its cluster picture will have at least two clusters of size 2 or 4 (Theorem 2.17).

Lemma 8.8. *Suppose that C has Type $\mathrm{I}^{\epsilon,\delta}_{n,m}$ or $\mathrm{I}^{\epsilon}_n\times\mathrm{I}^{\delta}_m$, and that $\widehat{C}$ has Type $\mathrm{I}^{\epsilon',\delta'}_{2n,2m}$ or $\mathrm{I}^{\epsilon'}_{2n}\times\mathrm{I}^{\delta'}_{2m}$. Then $\epsilon=\epsilon'$ and $\delta=\delta'$.*

Proof. Write C^+_k and C^-_k for the cyclic group C_k on which Frobenius acts trivially and by multiplication by -1, respectively. The Néron component group of $\mathrm{Jac}\,C/K^{nr}$ is $\Phi_C=C^{\epsilon}_n\times C^{\delta}_m$, and similarly for $\widehat{C}$ (see Remark 2.18). Passing to a quadratic ramified extension if necessary, we may assume that n and m are even.

The Richelot isogeny and its dual induce Frobenius-equivariant maps $f:\Phi_C\to\Phi_{\widehat{C}}$ and $g:\Phi_{\widehat{C}}\to\Phi_C$ such that both $f\circ g$ and $g\circ f$ are multiplication-by-2 maps. As $|\Phi_{\widehat{C}}|=4|\Phi_C|$, this forces f to be injective and g surjective with kernel $C_2\times C_2$. Hence, $\Phi_C\simeq(C^{\epsilon'}_{2n}\times C^{\delta'}_{2m})/C_2\times C_2\simeq C^{\epsilon'}_n\times C^{\delta'}_m$. By Remark 2.18, $\epsilon=\epsilon'$ and $\delta=\delta'$. □

Cases $\mathrm{I}^{\epsilon,\delta}_{n,m}$ (a) and $\mathrm{I}^{\epsilon}_{n\sim n}$ (a). Here $v(\Delta/c)=r\geqslant 0$. Proposition 8.4(1,2,3) gives $v(\hat{\alpha}_i-\hat{\beta}_i)=0$ for all i. In particular, there is no cluster of size $\geqslant 4$ and no two roots of the same colour lie in one cluster. It follows that the cluster picture of $\widehat{C}$ must be either  ,  ,  or  . The latter cannot in fact occur: otherwise, by Lemma 8.6 and

Proposition 8.4(7), we would have $0 = v(\frac{\Delta(\widehat{C})}{c(\widehat{C})}) = v(\frac{\Delta(\widehat{C})}{\ell_1\ell_2\ell_3/\Delta(C)}) = v(\frac{\Delta(C)^2}{c^2}) = 2r$, at which point Proposition 8.4(4) forces $v(s-t) = 0$ for each sapphire root s and turquoise root t, so that there is no sapphire–turquoise twin.

We may now relabel the roots $\hat{\alpha}_i \leftrightarrow \hat{\beta}_i$, so that the three leftmost roots in the given pictures are $\hat{\alpha}_1, \hat{\alpha}_2$ and $\hat{\alpha}_3$, in some order, so that $v(\hat{\alpha}_i - \hat{\beta}_j) = 0$ for all i, j. Proposition 8.4(4,5,6) gives

$$v((\hat{\alpha}_2 - \hat{\alpha}_3)(\hat{\beta}_2 - \hat{\beta}_3)) = 2r, \quad v((\hat{\alpha}_3 - \hat{\alpha}_1)(\hat{\beta}_3 - \hat{\beta}_1)) = 2r + n,$$

$$v((\hat{\alpha}_1 - \hat{\alpha}_2)(\hat{\beta}_1 - \hat{\beta}_2)) = 2r + m.$$

Hence, the cluster picture must be for some integer $0 \leqslant z \leqslant 2r$.

If C has type $\mathrm{I}^{\epsilon,\delta}_{n,m}$, Galois preserves $\{\alpha_2, \beta_2\}$ and $\{\alpha_3, \beta_3\}$, so that $\ell_1 \in K$ (see Definition 1.12). By Proposition 8.4(1) $(\hat{\alpha}_1 - \hat{\beta}_1)^2 = \frac{1}{4\ell_1^2}(\alpha_2 - \alpha_3)(\alpha_2 - \beta_3)(\beta_2 - \alpha_3)(\beta_2 - \beta_3)$, which is Galois-stable, a unit and a perfect square in the residue field, so $\hat{\alpha}_1 - \hat{\beta}_1 \in K$ and the two possible clusters of size 3 for $\widehat{C}$ are not interchanged by Galois. It follows from Lemma 8.8 that $\widehat{C}$ has cluster picture with Frobenius action  . Lemma 8.7 gives the required model for $\widehat{C}$.

Conversely, if C has type $\mathrm{I}^{\epsilon}_{n\sim n}$, then Frobenius swaps $\{\alpha_2, \beta_2\}$ and $\{\alpha_3, \beta_3\}$, so $\mathrm{Frob}(\ell_1) = -\ell_1$, and hence $\mathrm{Frob}(\hat{\alpha}_1 - \hat{\beta}_1) = \hat{\beta}_1 - \hat{\alpha}_1$, as above. Thus, $\widehat{C}$ has type $\mathrm{I}^{\epsilon}_{2n\sim 2n}$ or $\mathrm{I}^{\epsilon}_{2n}\tilde{\mathrm{x}}_r\mathrm{I}_{2n}$ by Lemma 8.5, and cluster picture with Frobenius action  .

Cases $\mathrm{I}^{\epsilon,\delta}_{n,m}$ (b) and $\mathrm{I}^{\epsilon}_{n\sim n}$(b). In these cases, $v(\Delta/c) = r + \frac{n}{2}$ and $v(\ell_1) = \frac{n}{2}$. Proposition 8.4 gives $v(\hat{\alpha}_1 - \hat{\beta}_1) = \frac{m-n}{4}$, $v(\hat{\alpha}_i - \hat{\beta}_i) = 0$ for $i = 2, 3$, and

$$v((\hat{\alpha}_2 - \hat{\alpha}_3)(\hat{\alpha}_2 - \hat{\beta}_3)(\hat{\beta}_2 - \hat{\alpha}_3)(\hat{\beta}_2 - \hat{\beta}_3)) = n + 2r,$$

$$v((\hat{\alpha}_3 - \hat{\alpha}_1)(\hat{\alpha}_3 - \hat{\beta}_1)(\hat{\beta}_3 - \hat{\alpha}_1)(\hat{\beta}_3 - \hat{\beta}_1)) = 2r,$$

$$v((\hat{\alpha}_1 - \hat{\alpha}_2)(\hat{\alpha}_1 - \hat{\beta}_2)(\hat{\beta}_1 - \hat{\alpha}_2)(\hat{\beta}_1 - \hat{\beta}_2)) = 2r.$$

First suppose that C is of type $\mathrm{I}^{\epsilon,\delta}_{n,m}$ for some $n < m$. Without loss of generality, $\alpha_2 \equiv \alpha_3 \bmod \pi_K^{m/2}$. This gives $\Delta/c \equiv (\beta_2 - \beta_3)(\alpha_1 - \alpha_2)(\beta_1 - \alpha_2) \bmod \pi_K^{m/2}$, so that Δ has valuation exactly $n/2$ and hence $r = 0$. The above expressions and the restriction on the type then force the cluster picture of $\widehat{C}$ to be  . Moreover, the sum of the depths of the sapphire–turquoise twins is n, and the explicit description of the roots in Lemma 8.3 shows that each depth is at least $n/2$, so that each must be exactly $n/2$.

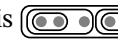
By Lemma 8.5, if $\epsilon = \delta$, then $\widehat{C}$ has type $\mathrm{U}^{\epsilon}_{\frac{m-n}{2},n,n}$ and hence cluster picture with Frobenius action  ; and if $\epsilon \neq \delta$, then $\widehat{C}$ either has type $\mathrm{U}^{\epsilon}_{\frac{m-n}{2},n\sim n}$ or $\mathrm{U}^{\delta}_{\frac{m-n}{2},n\sim n}$. In the latter case, the sign is determined by whether $\frac{\ell_1\ell_2\ell_3}{\Delta} \in K^{\times 2}$ or not (see Definition 2.13). Working modulo $\pi_K^{m/2}$, we have $\ell_1 \equiv \beta_2 - \beta_3$, $\ell_2 \equiv \alpha_2 + \beta_3$, $\ell_3 \equiv \alpha_2 + \beta_2$,

$$\Delta/c \equiv (\beta_2 - \beta_3)(\alpha_2 - \alpha_1)(\alpha_2 - \beta_1), \quad \theta^2_{\{\alpha_2,\alpha_3\}} \equiv c(\alpha_2 - \alpha_1)(\alpha_2 - \beta_1)(\alpha_2 - \beta_2)(\alpha_2 - \beta_3).$$

All of the factors in these expressions are units except for $\beta_2-\beta_3$, which has valuation exactly $\frac{n}{2}$ (as it is smaller than $\frac{m}{2}$). Dividing through by $\beta_2-\beta_3$ and then working modulo $\pi_K^{\min(\frac{m-n}{2},\frac{n}{2})}$ (so that also $\beta_2\equiv\beta_3$), we get

$$\frac{\Delta}{c\ell_1\ell_2\ell_3}\equiv\frac{(\alpha_2-\alpha_1)(\alpha_2-\beta_1)}{c(\alpha_2+\beta_2)^2}\equiv\frac{\theta^2_{\{\alpha_2,\alpha_3\}}}{c^2(\alpha_2-\beta_2)^2(\alpha_2+\beta_2)^2}.$$

Hence, $\frac{\Delta}{c\ell_1\ell_2\ell_3}=\square\cdot\theta^2_{\{\alpha_2,\alpha_3\}}$ in $K^{\times 2}$. Thus, the sign is the same as of the cluster $\{\alpha_2,\alpha_3\}$ for C, and $\widehat{C}$ has cluster picture with Frobenius action  .

Now suppose that the type is $\mathrm{I}^{\epsilon,\delta}_{n,n}$ or $\mathrm{I}^{\epsilon}_{n\sim n}$. As $v(\hat\alpha_i-\hat\beta_i)=0$, the same argument as for case $\mathrm{I}^{\epsilon,\delta}_{n,m}$(a) shows that the cluster picture of $\widehat{C}$ is  , or , in which the three leftmost roots have different colours, and similarly for the rightmost three (the fourth picture again cannot occur as it would yield $0=2v(\Delta)-v(\ell_1)=2r+\frac{n}{2}>0$). The average valuation of ● - ◆ (i.e. of a sapphire minus a turquoise root) is higher than that of ● - ◆, so at least one of the twins must consist of a sapphire and a turquoise root. The average valuation of ● - ◆ is the same as that of ● - ●, so both twins must be sapphire-turquoise, and the cluster picture is  for some $0\leqslant k\leqslant 2r$ and some $u,v>0$. For the two twins, from the valuations, we know that $u+v=n$. By Theorem 2.17, the Tamagawa numbers satisfy $c_{\mathrm{Jac}\,\widehat{C}/K^{nr}}=uv$ and $c_{\mathrm{Jac}\,C/K^{nr}}=n^2/4$, so that as the Richelot isogeny has degree 4, we necessarily have $uv=2^jn^2$ for some $j\in\mathbb{Z}$ (Lemma 3.4). A little exercise in elementary number theory shows that as $\frac{u}{n}+\frac{v}{n}=1$ and $\frac{u}{n}\cdot\frac{v}{n}=2^j$, it follows that $u=v=\frac{n}{2}$.

Frobenius will swap the two twins (and hence the two clusters of size 3) if and only if it swaps the residues of $\hat\alpha_2$ and $\hat\beta_2$. Working in the residue field, Proposition 8.4(2), Definition 2.13 and the cluster picture of C tell us that

$$\begin{aligned}(\hat\alpha_2-\hat\beta_2)^2&\equiv\frac{(\alpha_3-\alpha_1)(\alpha_3-\beta_1)(\beta_3-\alpha_1)(\beta_3-\beta_1)}{(\alpha_3+\beta_3)^2}\\&\equiv\frac{\theta^2_{\{\alpha_2,\beta_2\}}\theta^2_{\{\alpha_3,\beta_3\}}}{c^2(\alpha_3+\beta_3)^2(\alpha_3-\beta_3)^4}\equiv\square\cdot\theta^2_{\{\alpha_2,\beta_2\}}\theta^2_{\{\alpha_3,\beta_3\}}.\end{aligned}$$

Thus, Frobenius preserves the two twins of $\widehat{C}$ when C has type $\mathrm{I}^{+,+}_{n,n}$, $\mathrm{I}^{-,-}_{n,n}$ or $\mathrm{I}^{+}_{n\sim n}$, and swaps them for types $\mathrm{I}^{+,-}_{n,n}$ and $\mathrm{I}^{-}_{n\sim n}$. Together with Lemmata 8.5 and 8.7, this gives a model for $\widehat{C}$ with the desired cluster picture.

Cases $\mathrm{U}^{\epsilon}_{n,m,l}$ (a) and $\mathrm{U}^{\epsilon}_{n\sim n,l}$ (a). By Lemma 8.6(2), $v(\Delta/c)=0$. Also by Proposition 8.4(1,2,3) $v(\hat\alpha_i-\hat\beta_i)=0$ for all i, so, in particular, there is no cluster of size $\geqslant 4$ and a cluster of size 3 cannot contain two roots of the same colour. By Lemma 8.6(3) and Proposition 8.4(7), it follows that there is no cluster of size 3 either, since $v(\frac{\Delta(\widehat{C})}{c(\widehat{C})})=v(\frac{\Delta(\widehat{C})}{\ell_1\ell_2\ell_3/\Delta(C)})=v(\frac{\Delta(C)^2}{c^2})=0$. By Proposition 8.4(4,5,6),

$$v((\hat\alpha_2-\hat\alpha_3)(\hat\alpha_2-\hat\beta_3)(\hat\beta_2-\hat\alpha_3)(\hat\beta_2-\hat\beta_3))=n,$$

$$v((\hat\alpha_3-\hat\alpha_1)(\hat\alpha_3-\hat\beta_1)(\hat\beta_3-\hat\alpha_1)(\hat\beta_3-\hat\beta_1))=m,$$

$$v((\hat\alpha_1-\hat\alpha_2)(\hat\alpha_1-\hat\beta_2)(\hat\beta_1-\hat\alpha_2)(\hat\beta_1-\hat\beta_2))=l.$$

It follows that the cluster picture of $\widehat{C}$ is  .

The only twins that can be swapped by Frobenius are the ones containing the ruby roots. This happens if and only if $\mathrm{Frob}(\hat{\alpha}_1 - \hat{\beta}_1) = \hat{\beta}_1 - \hat{\alpha}_1$, which, by Proposition 8.4(1), is equivalent to $\mathrm{Frob}(\ell_1) = -\ell_1$. It follows that the two twins for $\widehat{C}$ are swapped when C is in case $\mathrm{U}^{\epsilon}_{n\sim n,l}(a)$, and not swapped in case $\mathrm{U}^{\epsilon}_{n,m,l}(a)$. The sign for $\widehat{C}$ is determined by whether $\frac{\ell_1\ell_2\ell_3}{\Delta}$ is a square (see Definition 2.13). As $\alpha_1 \equiv 0, \alpha_2 \equiv \beta_2$ and $\alpha_3 \equiv \beta_3$, we have that $\frac{\ell_1\ell_2\ell_3}{\Delta} \equiv \frac{8(\alpha_2-\alpha_3)\alpha_2\alpha_3}{c(2\alpha_2^2\alpha_3-2\alpha_3^2\alpha_2)} \equiv \frac{4}{c}$ in the residue field, so this is the same as the sign for C.

Cases $\mathrm{I}^{\epsilon}_n \times_t \mathrm{I}^{\delta}_m(\mathrm{a})$ and $\mathrm{I}^{\epsilon}_n \tilde{\times}_t \mathrm{I}_n\,(\mathrm{a})$. By Lemma 8.6 $v(\Delta/c) = 0$. Also Proposition 8.4(1,4) gives $v(\hat{\alpha}_1 - \hat{\beta}_1) = v((\hat{\alpha}_2 - \hat{\alpha}_3)(\hat{\alpha}_2 - \hat{\beta}_3)(\hat{\beta}_2 - \hat{\alpha}_3)(\hat{\beta}_2 - \hat{\beta}_3)) = 0$, so, in particular, there can be no cluster of size $\geqslant 4$. Moreover, Proposition 8.4(2,3) gives $v(\hat{\alpha}_2 - \hat{\beta}_2) = v(\hat{\alpha}_3 - \hat{\beta}_3) = t$, so the two sapphire roots lie in a non-trivial cluster, as do the two turquoise roots, and hence, $\widehat{C}$ cannot have three twins. Thus, the possible cluster pictures for $\widehat{C}$ are  ,  ,  and  , where the three leftmost roots are the two sapphire ones and a ruby one, in some order. Proposition 8.4(5,6) gives

$$v((\hat{\alpha}_3-\hat{\alpha}_1)(\hat{\alpha}_3-\hat{\beta}_1)(\hat{\beta}_3-\hat{\alpha}_1)(\hat{\beta}_3-\hat{\beta}_1))=n+2t,$$

$$v((\hat{\alpha}_1-\hat{\alpha}_2)(\hat{\alpha}_1-\hat{\beta}_2)(\hat{\beta}_1-\hat{\alpha}_2)(\hat{\beta}_1-\hat{\beta}_2))=m+2t,$$

which forces the cluster picture of $\widehat{C}$ to be  .

The same argument as in cases $\mathrm{I}^{\epsilon,\delta}_{n,m}$ and $\mathrm{I}^{\epsilon}_{n\sim n}$, shows that for case $\mathrm{I}^{*}_{2n} \times_t \mathrm{I}^{*}_{2m}$, the cluster picture with Frobenius action of $\widehat{C}$ is  , and for case $\mathrm{I}^{\epsilon}_n \tilde{\times}_t \mathrm{I}_n$, it is  .

This completes the proof of Theorem 8.1.

9 | ODD PLACES: $\lambda_{C/K} w_{C/K} = E_{C/K}$

In this section, we will complete the proof of Theorem 7.1 by justifying the values it gives for $E_{C/K}$ and showing that $\lambda_{C/K} w_{C/K} = E_{C/K}$. Throughout we will use the division into cases as in Theorem 7.1.

Theorem 9.1. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \Delta, \eta_1 \neq 0$. Suppose that the cluster picture with Frobenius action of C is one of the cases in Theorem 7.1 and that*

- $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ *in cases* $1^{\epsilon}_n(a,b)$, $1^{\epsilon}_{2n}(c,d)$ *and* $1 \times_t \mathrm{I}^{\epsilon}_n(a)$,
- $v(\ell_1) = v(\ell_2) = v(\ell_3) = 0$ *in cases* $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$, $\mathrm{I}^{\epsilon}_{n\sim n}(a)$,
- $v(\ell_1) = t$ *in cases* $1\times_t 1(b,c)$ *and* $1\tilde{\times}_t 1(b,c)$, *and*
- $v(\ell_1) = \frac{n}{2}$, $v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ *in cases* $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$ *and* $\mathrm{I}^{\epsilon}_{n\sim n}(b)$.

Then $E_{C/K}$ is as given in Theorem 7.1, and $E_{C/K} = \lambda_{C/K} w_{C/K}$.

Proof. Combine Lemmata 9.4, 9.5, 9.6, 9.7, 9.10, 9.11 and 9.12 below. □

The remainder of this section is devoted to the proof of this result. Throughout the section, $K/\mathbb{Q}_p$ will be a finite extension for an odd prime p and C/K will be a centred semistable C2D4 curve with $\mathcal{P}, \Delta, \eta_1 \neq 0$.

9.1 | The value of $\lambda_{C/K} w_{C/K}$

Here we convert $\lambda_{C/K} w_{C/K}$ into Hilbert symbols. As both $\lambda_{C/K}$ and $w_{C/K}$ are sensitive to the signs of twins, we first express these signs (defined via $\theta^2_{\mathfrak{t}}$, see Definition 2.13) in terms of our standard invariants from Definition 1.12.

Lemma 9.2. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \eta_1, \Delta \neq 0$. For a twin cluster $\mathfrak{t}$, $\theta^2_{\mathfrak{t}}$ satisfies the following equalities:*

(1) *In case* $1^{\epsilon}_n(a)$ ($\overset{\epsilon}{n/2}\bullet\bullet\bullet\bullet$): $\theta^2_{\mathfrak{t}} = c\xi\square$.
(2) *In case* $1_n(b)$ ($\overset{\epsilon}{n/2}\bullet\bullet\bullet\bullet$): $\theta^2_{\mathfrak{t}} = c\eta_1\eta_2\square$.
(3) *In case* $1_{2n}(c)$ ($\overset{\epsilon}{n}\bullet\bullet\bullet\bullet$): $\theta^2_{\mathfrak{t}} = -\frac{\ell_1}{\Delta}\eta_1\square$.
(4) *In case* $1_{2n}(d)$ ($\overset{\epsilon}{n}\bullet\bullet\bullet\bullet$): $\theta^2_{\mathfrak{t}} = -2c\xi\hat{\delta}_2\eta_2\square$.
(5) *In case* $I^{\epsilon,\delta}_{n,m}(a)$ ($\overset{\epsilon}{n/2}\overset{\delta}{m/2}\bullet\bullet$): $\theta^2_{\mathfrak{t}_2} = 2c\eta_2\square$ *and* $\theta^2_{\mathfrak{t}_3} = 2c\eta_3\square$.
(6) *In case* $I^{\epsilon}_{n\sim n}(a)$ ($\overset{+}{n/2}\overset{\epsilon}{n/2}\bullet\bullet$): $\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3} = \eta_2\eta_3\square$.
(7) *In cases* $I^{\epsilon,\delta}_{n,m}(b)$ ($\overset{\epsilon}{n/2}\overset{\delta}{m/2}\bullet\bullet$) *and* $I^{\epsilon}_{n\sim n}(b)$ ($\overset{+}{n/2}\overset{\epsilon}{n/2}\bullet\bullet$):
if $n < m$, then $\theta^2_{\mathfrak{t}_\beta} = \frac{\ell_1}{\Delta}\square$,
for any n, m, $\theta^2_{\mathfrak{t}_\alpha}\theta^2_{\mathfrak{t}_\beta} = -\eta_1(\delta_2\eta_2 + \delta_3\eta_3)(\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2)\square$.
(8) *In case* $1\times_t I_n(a)$ ($\overset{\epsilon}{n/2}\ t\ \bullet\bullet$): $\theta^2_{\mathfrak{t}} = c\xi\square$.
(9) *In case* $I^{\epsilon}_n\times_t I^{\delta}_m(a)$ ($\overset{\epsilon}{n/2}\ t\ \overset{\delta}{m/2}\ t\ M$): $\theta^2_{\mathfrak{t}_2} = 2c\eta_2\square$ *and* $\theta^2_{\mathfrak{t}_3} = 2c\eta_3\square$.
(10) *In case* $I^{\epsilon}_n\tilde{\times}_t I_n(a)$ ($\overset{+}{n/2}\ t\ \overset{\epsilon}{n/2}\ t$): $\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3} = \eta_2\eta_3\square$.

Here in (5), (6), (9), (10), $\mathfrak{t}_2 = \{\alpha_2, \beta_2\}$ and $\mathfrak{t}_3 = \{\alpha_3, \beta_3\}$, and in (7), $\mathfrak{t}_\alpha = \{\alpha_2, \alpha_3\}$ is the left twin and $\mathfrak{t}_\beta = \{\beta_2, \beta_3\}$ is the right twin.

Proof. We will write k for the residue field of K, $x \to \bar{x}$ for the reduction map to $\bar{k}$, and $\equiv$ for equality in the residue field (unless specified otherwise). In each case, we will show that, after a suitable scaling to make both sides units, the claimed identities hold over the residue field. The result then follows by Hensel's lemma.

(1) Here $\alpha_1 \equiv -\alpha_1 \equiv 0$, and $\frac{4}{c}\theta^2_{\mathfrak{t}} \equiv 4\alpha_2\beta_2\alpha_3\beta_3 \equiv \xi$ are units; also $\xi, \theta^2_{\mathfrak{t}} \in K$.
(2) Here $\frac{4}{c}\theta^2_{\mathfrak{t}} \equiv 4(\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\alpha_2-\alpha_3)(\alpha_2-\beta_3) \equiv \eta_1\eta_2$ are units, and $\eta_1, \eta_2, \theta^2_{\mathfrak{t}} \in K$.
(3) Let $\mathfrak{t} = \{\alpha_2, \alpha_3\}$. Then $\frac{1}{c}\theta^2_{\mathfrak{t}} \equiv (\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\alpha_2-\beta_2)(\alpha_2-\beta_3)$, $\ell_1 \equiv \beta_2 - \beta_3$, $\eta_1 \equiv (\beta_2 - \alpha_2)(\alpha_2 - \beta_3)$ and $\Delta/c \equiv (\beta_2-\beta_3)(\alpha_2-\alpha_1)(\alpha_2+\alpha_1)$. Hence $\frac{1}{c}\theta^2_{\mathfrak{t}} \equiv -\frac{\ell_1}{\Delta/c}\eta_1(\alpha_2-\alpha_1)^2(\alpha_2+\alpha_1)^2$ are units, which gives the result as $\theta^2_{\mathfrak{t}}, \frac{\ell_1}{\Delta}, \eta_1 \in K$ and $(\bar{\alpha}_2 - \bar{\alpha}_1)(\bar{\alpha}_2 + \bar{\alpha}_1) \in k^\times$.
(4) Let $\mathfrak{t} = \{\alpha_1, \alpha_2\}$. Then $\frac{1}{c}\theta^2_{\mathfrak{t}} \equiv 2\alpha_1(\alpha_1-\beta_2)(\alpha_1-\alpha_3)(\alpha_1-\beta_3)$, $\hat{\delta}_2 \equiv 4(\alpha_3+\alpha_1)(\alpha_3-\alpha_1)\cdot(\beta_3+\alpha_1)(\beta_3-\alpha_1)$, $\xi \equiv 4\alpha_1(\alpha_1+\beta_2)(\alpha_1+\alpha_3)(\alpha_1+\beta_3)$ and $\eta_2 \equiv (\beta_2 - \alpha_1)(\beta_2 + \alpha_1)$. Hence $\frac{16}{c}\theta^2_{\mathfrak{t}}(\alpha_1+\beta_2)^2(\alpha_1+\alpha_3)^2(\alpha_1+\beta_3)^2 \equiv -2\xi\hat{\delta}_2\eta_2$, which gives the results as $\theta^2_{\mathfrak{t}}, \xi, \hat{\delta}_2, \eta_2 \in K$ and $(\bar{\alpha}_1+\bar{\beta}_2), (\bar{\alpha}_1+\bar{\alpha}_3)(\bar{\alpha}_1+\bar{\beta}_3) \in k^\times$.
(5, 6) Here $\frac{4}{c}\theta^2_{\mathfrak{t}_2} \equiv 4(\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\alpha_2-\alpha_3)^2 \equiv 2\eta_2(\alpha_2-\alpha_3)^2$ are units. For (5), $\theta^2_{\mathfrak{t}_2}, \eta_2 \in K$ and $(\bar{\alpha}_2 - \bar{\alpha}_3) \in k^\times$. The argument for $\mathfrak{t}_3$ is similar. For (6), we obtain $\frac{4}{c^2}\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3} \equiv 4(\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\alpha_3-\alpha_1)(\alpha_3+\alpha_1)(\alpha_2-\alpha_3)^4 \equiv \eta_2\eta_3(\alpha_2-\alpha_3)^4$ units, with $\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3}, \eta_2\eta_3 \in K$ and $(\bar{\alpha}_2-\bar{\alpha}_3)^2 \in k^\times$.

(7) Here $\frac{1}{c}\theta^2_{\mathfrak{t}_\beta} \equiv (\beta_2-\alpha_1)(\beta_2+\alpha_1)(\beta_2-\alpha_2)^2$. Also $\ell_1 \equiv \alpha_2-\alpha_3 \bmod \pi_K^{m/2}$ and $\Delta/c \equiv (\alpha_2-\alpha_3)(\beta_2-\alpha_1)(\beta_2+\alpha_1) \bmod \pi_K^{m/2}$.

If $n<m$, then $v(\ell_1)=v(\Delta/c)=\frac{n}{2}$ and $\frac{\Delta}{c\ell_1} \equiv (\beta_2-\alpha_1)(\beta_2+\alpha_1)$. Thus, $\frac{1}{c}\theta^2_{\mathfrak{t}_\beta} \equiv \frac{\Delta}{c\ell_1}\cdot(\beta_2-\alpha_2)^2$ are units with $\theta^2_{\mathfrak{t}_\beta}, \frac{\Delta}{\ell_1} \in K$ and $(\bar\beta_2-\bar\alpha_2)\in k^\times$.

In general, $\frac{4}{c^2}\theta^2_{\mathfrak{t}_\alpha}\theta^2_{\mathfrak{t}_\beta}(\alpha_2-\beta_2)^4 \equiv 4(\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\beta_2-\alpha_1)(\beta_2+\alpha_1)(\alpha_2-\beta_2)^8 \equiv -\eta_1(\delta_2\eta_2+\delta_3\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2)$. This gives the second claim as $\theta^2_{\mathfrak{t}_\alpha}\theta^2_{\mathfrak{t}_\beta}, \eta_1, (\delta_2\eta_2+\delta_3\eta_3), (\hat\delta_2\eta_3+\hat\delta_3\eta_2) \in K$ and $(\bar\alpha_2-\bar\beta_2)^2\in k^\times$.

(8) Here $\alpha_1 \equiv -\alpha_1 \equiv 0 \bmod \pi_K^{t+\frac{n}{2}}$, so that $\frac{4}{c}\theta^2_{\mathfrak{t}} \equiv 4\alpha_2\beta_2\alpha_3\beta_3 \equiv \xi \bmod \pi_K^{t+\frac{n}{2}}$. As $v(\beta_2)=v(\alpha_3)=v(\beta_3)=0$ and $v(\alpha_2)=t$, it follows that $\frac{4\theta^2_{\mathfrak{t}}}{c\xi} \equiv 1$, which gives the result as $\theta^2_{\mathfrak{t}}, \xi \in K$.

(9, 10) Here $\frac{1}{c}\theta^2_{\mathfrak{t}_2} \equiv (\alpha_2-\alpha_1)(\alpha_2+\alpha_1)(\alpha_2-\alpha_3)(\alpha_2-\beta_3) \bmod \pi_K^{t+\frac{n}{2}}$ and $\eta_2 \equiv 2(\alpha_2-\alpha_1)\cdot(\alpha_2+\alpha_1) \bmod \pi_K^{t+\frac{n}{2}}$. As $v(\alpha_2-\alpha_1)=t$, the other factors are units and $-\alpha_1 \equiv \alpha_3 \equiv \beta_3$ we obtain $\frac{2}{c(\alpha_2-\alpha_1)}\theta^2_{\mathfrak{t}_2} \equiv 2(\alpha_2+\alpha_1)^3 \equiv \frac{\eta_2}{(\alpha_2-\alpha_1)}(\alpha_2+\alpha_1)^2$ are units, and hence $\frac{2}{c\eta_2}\theta^2_{\mathfrak{t}_2} \equiv (\alpha_2+\alpha_1)^2$. This gives the result for (9) as $\theta^2_{\mathfrak{t}_2}, \eta_2 \in K$ and $(\bar\alpha_2+\bar\alpha_1)\in k^\times$, with a similar proof for $\theta^2_{\mathfrak{t}_3}$. For (10), we obtain $\frac{4}{c^2\eta_2\eta_3}\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3} \equiv (\alpha_2+\alpha_1)^4$ with $\theta^2_{\mathfrak{t}_2}\theta^2_{\mathfrak{t}_3}, \eta_2\eta_3 \in K$ and $(\bar\alpha_2+\bar\alpha_1)^2\in k^\times$. □

Lemma 9.3. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\ell_1,\ell_2,\ell_3,\Delta\neq 0$. Then*

- $\hat\delta_1 \in K^{\times 2}$ *if and only if* $(\hat\alpha_1-\hat\beta_1)^2 \in K^{\times 2}$,
- $\hat\delta_1 \notin K^{\times 2}$ *in case* $1\tilde{\times}1(a)$,
- $\hat\delta_1 \notin K^{\times 2}$ *in case* $\mathrm{I}^{\epsilon}_n\tilde{\times}_t\mathrm{I}_n(a)$,
- $\hat\delta_1 \in K^{\times 2}$ *if and only if* $\epsilon\delta=+$ *in case* $\mathrm{I}^{\epsilon,\delta}_{n,n}(b)$,
- $\hat\delta_1 \in K^{\times 2}$ *if and only if* $\epsilon=+$ *in case* $\mathrm{I}^{\epsilon}_{n\sim n}(b)$.

Moreover, in the last four cases, $\hat\delta_1$ has even valuation.

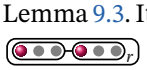
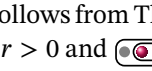
Proof. Taking an odd degree unramified extension, we may assume that $|k|\geqslant 23$. By Proposition 8.4(1), $\hat\delta_1 = \frac{\ell_1^2}{\Delta^2}(\hat\alpha_1-\hat\beta_1)^2 = \square(\hat\alpha_1-\hat\beta_1)^2 = \square\delta_1(\widehat{C})$ since $\frac{\ell_1}{\Delta}\in K$. By Theorem 8.1, $\widehat{C}$ admits a model $\widehat{C}'$ whose cluster picture is the one given in the table of Theorem 7.1. By Remark 6.2, we can write $\widehat{C}'=\widehat{C}_m$ for a Möbius transformation $m(x)=\frac{\mathbf{a}x+\mathbf{b}}{\mathbf{c}x+\mathbf{d}}$ as in Definition 6.1. We explicitly compute $\delta_1(\widehat{C}_m) = \frac{(\hat\alpha_1-\hat\beta_1)^2(\mathbf{ad}-\mathbf{bc})^2}{(\mathbf{c}\hat\alpha_1+\mathbf{d})^2(\mathbf{c}\hat\beta_1+\mathbf{d})^2} = (\hat\alpha_1-\hat\beta_1)^2\square = \delta_1(\widehat{C})\square$. Therefore, it is sufficient to check the valuation of $\hat\alpha_1-\hat\beta_1$ and whether $\hat\alpha_1-\hat\beta_1$ is preserved by the action of Galois on the picture of $\widehat{C}$ in the table of Theorem 7.1. □

Lemma 9.4. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P},\eta_1,\Delta\neq 0$. Suppose that the cluster picture of C is* *(cases 2(a, d)),*

 *(cases 2(b, e)), or*  *(cases 2(c, f)). Then*

$$\lambda_{C/K} w_{C/K} = \left\{ \begin{array}{ll} 1 & \text{if } \hat\delta_1 = \square \\ (-1)^r & \text{if } \hat\delta_1 \neq \square \end{array} \right\} = \left\{ \begin{array}{ll} (\hat\delta_1, -\frac{\ell_1}{\Delta}) & \text{cases 2 } (a,b,d,e), \\ (\hat\delta_1, -c\frac{\ell_1}{\Delta}) & \text{cases 2 } (c,f). \end{array} \right.$$

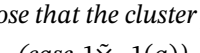
Proof. The first equality follows from Theorem 7.1. The second equality is clear in cases 2(a,b,c), so suppose that C is as in cases 2(d,e,f). Note that $\hat\delta_1 = \frac{1}{\Delta^2}(\alpha_2-\beta_3)(\alpha_2-\alpha_3)(\beta_2-\alpha_3)(\beta_2-\beta_3)$ has even valuation, so it will suffice to show that $v(\frac{\ell_1}{\Delta}) \equiv r \bmod 2$ in cases 2(d,e) and $v(\frac{\ell_1}{\Delta}) \equiv r + v(c) \bmod 2$ in case 2(f).

Since $\hat\delta_1 \neq \square$, some Galois element swaps $\hat\alpha_1$ and $\hat\beta_1$ by Lemma 9.3. It follows from Theorems 7.1 and 2.17 that $\widehat{C}$ has cluster picture with Frobenius action  if $r > 0$ and  for some $m \geqslant 0$ if $r = 0$ (with $m = 0$ if and only if the five roots do not form a cluster).

Let $D = \Sigma_{x,x'} v(x-x')$, the sum taken over $x \in \{\hat\alpha_1, \hat\beta_1\}$ and $x' \in \{\hat\alpha_2, \hat\beta_2, \hat\alpha_3, \hat\beta_3\}$; it follows from the cluster pictures that $D = 6m$ if $r = 0$ and $D = 4r$ if $r > 0$. The result follows by combining the following equalities:

- $v(\frac{\ell_1}{\Delta}) + v(\ell_2\ell_3) = v(\frac{\ell_1\ell_2\ell_3}{\Delta}) \equiv r + \left\{ \begin{array}{ll} m & \text{if } r{=}0 \\ 0 & \text{if } r{>}0 \end{array} \right. \bmod 2$ (Theorem 2.12(3) for $\widehat{C}$),
- $v(\delta_2\delta_3) = v(\frac{c^4\ell_1^4}{\Delta^4}\ell_2^2\ell_3^2) + D \equiv 2v(\ell_2\ell_3) + \left\{ \begin{array}{ll} 2m & \text{if } r{=}0 \\ 0 & \text{if } r{>}0 \end{array} \right. \bmod 4$ (Proposition 8.4(5,6)),
- $v(\delta_2\delta_3) \equiv \left\{ \begin{array}{ll} 0 & \text{cases 2(d,e)} \\ 2k & \text{case 2(f)} \end{array} \right. \bmod 4$ (Definition 1.12),
- $v(c) \equiv k \bmod 2$ (Theorem 2.12(3) for C).

□

Lemma 9.5. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \eta_1, \Delta \neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(case $1\times_t 1(a)$),*  *(case $1\tilde\times_t 1(a)$),*  *(cases $1\times_t 1(b,c)$) or*  *(cases $1\tilde\times_t 1(b,c)$). Suppose moreover that $v(\ell_1) = t$ in cases $1\times_t 1(b,c)$ and $1\tilde\times_t 1(b,c)$. Then*

$$\lambda_{C/K} w_{C/K} = \left\{ \begin{array}{ll} 1 & \text{cases } 1\times_t 1(a,b) \text{ and } 1\tilde\times_t 1(a) \\ (-1)^r & \text{cases } 1\times_t 1(c) \\ (-1)^t & \text{cases } 1\tilde\times_t 1(b) \\ (-1)^{t+r} & \text{cases } 1\tilde\times_t 1(c) \end{array} \right\} = (c, \delta_1)\left(\hat\delta_1, -\frac{\ell_1}{\Delta}\right).$$

Proof. The first equality follows from Theorem 7.1.

Case $1\times_t 1$ (a). Galois fixes α_1 and does not permute colours, so $\alpha_1, \Delta \in K$ and $\delta_1, \hat\delta_1 \in K^{\times 2}$.

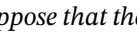
Case $1\tilde\times_t 1$ (a). Here $\delta_1, \hat\delta_1 \notin K^{\times 2}$ and both have even valuation by Lemma 9.3, so $\hat\delta_1 = \delta_1 \cdot \square$. Moreover, here $v(\ell_1) = 0$ and $v(\Delta/c) = 0$ by Lemma 8.6(1), so $(c,\delta_1)(-\frac{\ell_1}{\Delta}, \hat\delta_1) = (c\ell_1/\Delta, \delta_1) = 1$, as both terms have even valuation.

Cases $1\times_t 1$ (b,c) and $1\tilde\times_t 1$ (b,c). Note that $v(c) \equiv t \bmod 2$ by Theorem 2.12(3). As $v(\delta_1)$ is even,

$$(c,\delta_1) = \left\{ \begin{array}{ll} 1 & \delta_1 \in K^{\times 2} \\ (-1)^t & \delta_1 \notin K^{\times 2} \end{array} \right. = \left\{ \begin{array}{ll} 1 & \text{case } 1\times_t 1(b,c) \\ (-1)^t & \text{case } 1\tilde\times_t 1(b,c) \end{array} \right.$$

Similarly, as $v(\hat{\delta}_1)$ is even and $v(\ell_1/\Delta)=v(\ell_1)-v(\Delta/c)+v(c)\equiv t-(2t+r)+t\equiv r \bmod 2$,

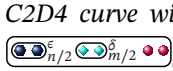
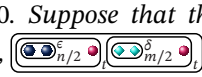
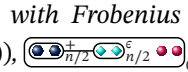
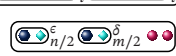
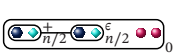
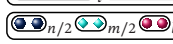
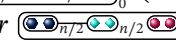
$$(\hat{\delta}_1,-\ell_1/\Delta)=\begin{cases}1 & \hat{\delta}_1\in K^{\times 2}\\ (-1)^{v(\ell_1/\Delta)} & \hat{\delta}_1\notin K^{\times 2}\end{cases}=\begin{cases}1 & \text{cases } 1\times_t 1(b),1\tilde{\times}_t 1(b)\\ (-1)^r & \text{cases } 1\times_t 1(c),1\tilde{\times}_t 1(c)\end{cases}.$$ □

Lemma 9.6. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P},\eta_1,\Delta\neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(case $1^{\epsilon}_n(a)$),*  *(case $1\times_t \mathrm{I}^{\epsilon}_n(a)$),*  *(case $1^{\epsilon}_n(b)$),*  *(case $1^{\epsilon}_{2n}(c)$), or*  *(case $1^{\epsilon}_{2n}(d)$). Then*

$$\lambda_{C/K}w_{C/K}=(\pm 1)^n=\begin{cases}(\delta_1,c\xi) & \text{cases } 1^{\pm}_n(a),1\times_t \mathrm{I}^{\pm}_n(a),\\ (\delta_2,c\eta_1\eta_2) & \text{cases } 1^{\pm}_n(b),\\ (\hat{\delta}_1,-\frac{\ell_1}{\Delta}\eta_1) & \text{cases } 1^{\pm}_{2n}(c),\\ (\hat{\delta}_3,-2c\xi\hat{\delta}_2\eta_2) & \text{cases } 1^{\pm}_{2n}(d).\end{cases}$$

Proof. The first equality follows from Theorem 7.1.

In case $1^{\pm}_n$(a), the cluster picture shows that $n=v(\delta_1)$, and Lemma 9.2(1) that the sign $\pm$ is determined by whether $\theta^2_{\{\alpha_1,-\alpha_1\}}=c\xi\square$ is a square in K. As $\theta^2_{\{\alpha_1,-\alpha_1\}}$ has even valuation (Remark 2.14), it follows that $(\pm 1)^n=(\delta_1,c\xi)$, as required. The other cases follow similarly, observing that $n=v(\delta_2),v(\hat{\delta}_1)-2v(\Delta),v(\hat{\delta}_3)$ or $v(\delta_1)-2t$, and that the sign is determined by whether $c\eta_1\eta_2,-\frac{\ell_1}{\Delta}\eta_1,-2c\xi\hat{\delta}_2\eta_2$ or $c\xi$ is a square in K for cases $1^{\pm}_n$(b), $1^{\pm}_{2n}$(c), $1^{\pm}_{2n}$(d) and $1\times_t \mathrm{I}^{\pm}_n$(a), respectively. (For $1^{\pm}_{2n}$(c), $v(\Delta)\in\mathbb{Z}$ as $v(\Delta/c)=0$ by Lemma 8.6.) □

Lemma 9.7. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P},\eta_1,\Delta\neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(case $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$),*  *(case $\mathrm{I}^{\epsilon}_n\times_t \mathrm{I}^{\delta}_m(a)$),*  *(case $\mathrm{I}^{\epsilon}_{n\sim n}(a)$),*  *($\mathrm{I}^{\epsilon}_n\tilde{\times}_t\mathrm{I}_n(a)$),*  *(case $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$),*  *(case $\mathrm{I}^{\epsilon}_{n\sim n}(b)$),*  *(case $\mathrm{U}^{\epsilon}_{n,m,l}(a)$) or*  *(case $\mathrm{U}^{\epsilon}_{n\sim n,l}(a)$). Moreover, suppose that $v(\ell_1)=\frac{n}{2}$ in cases $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$ and $\mathrm{I}^{\epsilon}_{n\sim n}(b)$. Then*

$$\lambda_{C/K}w_{C/K}=$$

$$\begin{cases}\epsilon^n\delta^m\\ \epsilon^n\delta^m\\ \epsilon^n(-1)^r\\ \epsilon^n\\ \epsilon^{n+r}\delta^{\frac{m+n}{2}+r}\\ \epsilon^{n+r}(-1)^n\\ \epsilon^{n+m+l}\\ \epsilon^l\end{cases}=\begin{cases}(\delta_2,2c\eta_2)(\delta_3,2c\eta_3) & \text{case } \mathrm{I}^{\epsilon,\delta}_{n,m}(a),\\ (\delta_2,2c\eta_2)(\delta_3,2c\eta_3) & \text{case } \mathrm{I}^{\epsilon}_n\times_t \mathrm{I}^{\delta}_m(a),\\ (\pi_K^r,\hat{\delta}_1)(\pi_K^n,\eta_2\eta_3) & \text{case } \mathrm{I}^{\epsilon}_{n\sim n}(a),\\ (\pi_K^n,\eta_2\eta_3) & \text{case } \mathrm{I}^{\epsilon}_n\tilde{\times}_t\mathrm{I}_n(a),\\ (\pi_K^n,-2\eta_1(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2))(\hat{\delta}_1,\frac{\ell_1}{\Delta}) & \text{case } \mathrm{I}^{\epsilon,\delta}_{n,m}(b),\\ (\pi_K^n,-2\eta_1(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2))(\hat{\delta}_1,\frac{\ell_1}{\Delta}) & \text{case } \mathrm{I}^{\epsilon}_{n\sim n}(b),\\ (\delta_1\delta_2\delta_3,c) & \text{case } \mathrm{U}^{\epsilon}_{n,m,l}(a),\\ (\delta_1,c) & \text{case } \mathrm{U}^{\epsilon}_{n\sim n,l}(a).\end{cases}$$

Proof. The first equality follows from Theorem 7.1.

Cases $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$, $\mathrm{I}^{\epsilon}_{n} \times_t \mathrm{I}^{\delta}_{m}(a)$: here $v(\delta_2) = n + 2t$ and $v(\delta_3) = m + 2t$ (with $t = 0$ for $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$). Also $\epsilon = +$ if and only if $\theta^2_{\{\alpha_2,\beta_2\}} = 2c\eta_2\square \in K^{\times 2}$, by Lemma 9.2(5). Similarly, $\delta = +$ if and only if $\theta^2_{\{\alpha_3,\beta_3\}} = 2c\eta_3\square \in K^{\times 2}$, by Lemma 9.2(5). The results follows since $\theta^2_{\{\alpha_2,\beta_2\}}$ and $\theta^2_{\{\alpha_3,\beta_3\}}$ have even valuations by Remark 2.14.

Case $\mathrm{I}^{\epsilon}_{n\sim n}$(a): here $\epsilon = +$ if and only if $\theta^2_{\{\alpha_2,\beta_2\}}\theta^2_{\{\alpha_3,\beta_3\}} = \eta_2\eta_3\square \in K^{\times 2}$, by Lemma 9.2(6). Also $\hat{\delta}_1 \notin K^{\times 2}$ by Lemma 9.3. The result follows as $v(\hat{\delta}_1) = 0$ and $\theta^2_{\{\alpha_2,\beta_2\}}$ and $\theta^2_{\{\alpha_3,\beta_3\}}$ have even valuations by Remark 2.14.

Case $\mathrm{I}^{\epsilon}_{n}\tilde{\times}_l\mathrm{I}_n$(a): here $\epsilon = +$ if and only if $\theta^2_{\{\alpha_2,\beta_2\}}\theta^2_{\{\alpha_3,\beta_3\}} = \eta_2\eta_3\square \in K^{\times 2}$, by Lemma 9.2(10).

Cases $\mathrm{I}^{\epsilon,\delta}_{n,m}$(b) and $\mathrm{I}^{\epsilon}_{n\sim n}$(b): write the right-hand side as $(\pi_K^n, 2(\delta_2+\delta_3)) \cdot (\pi_K^n, -\eta_1(\delta_2\eta_2 + \delta_3\eta_3) \cdot (\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2))(\hat{\delta}_1, \frac{\ell_1}{\Delta})$. From the cluster picture $2(\delta_2+\delta_3)$ is a square in the first case, and a non-square unit in the second case. So, $(\pi_K^n, 2(\delta_2+\delta_3)) = 1$ for $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$, and $(\pi_K^n, 2(\delta_2+\delta_3)) = (-1)^n$ for $\mathrm{I}^{\epsilon}_{n\sim n}$(b). By Lemma 9.2(7), $\theta^2_{\{\alpha_2,\alpha_3\}}\theta^2_{\{\beta_2,\beta_3\}} = -\eta_1(\delta_2\eta_2 + \delta_3\eta_3)(\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2)\square$ is a square if and only if $\epsilon\delta = +$ in the first case, and if and only if $\epsilon = +$ in the second case. In summary,

$$(\pi_K^n, -2\eta_1(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2)) = \begin{cases} \epsilon^n\delta^n & \text{case } \mathrm{I}^{\epsilon,\delta}_{n,m}(\mathrm{b}) \\ \epsilon^n(-1)^n & \text{case } \mathrm{I}^{\epsilon}_{n\sim n}(\mathrm{b}). \end{cases}$$

Also $v(\Delta) = v(c) + \frac{n}{2} + r \equiv \frac{n}{2} + r \bmod 2$ by the semistability criterion (Theorem 2.12), so that $v(\frac{\ell_1}{\Delta}) \equiv r \bmod 2$ and $v(\hat{\delta}_1) = v(\Delta^2\hat{\delta}_1) - 2v(\Delta) \equiv \frac{m-n}{2} \bmod 2$ (with $n = m$ in the case $\mathrm{I}^{\epsilon}_{n\sim n}$(b)). If $n < m$, without loss of generality $\alpha_2 \equiv \alpha_3 \bmod \pi_K^{m/2}$. This gives $\Delta/c \equiv (\beta_2-\beta_3)(\alpha_1-\alpha_2)\cdot(\beta_1-\alpha_2) \bmod \pi_K^{m/2}$, so that Δ has valuation exactly $n/2$ and hence $r = 0$ so $(\hat{\delta}_1, \frac{\ell_1}{\Delta}) = (\pi_K^{\frac{m-n}{2}}, \frac{\ell_1}{\Delta}) = \delta^{\frac{m-n}{2}}$ by Lemma 9.2(7). Conversely if $n = m$, then $(\hat{\delta}_1, \frac{\ell_1}{\Delta}) = (\pi_K^r, \hat{\delta}_1)$. By Lemma 9.3, $\hat{\delta}_1$ is a square if and only if $\epsilon\delta = +$ in the case $\mathrm{I}^{\epsilon,\delta}_{n,m}$(b), and if and only if $\epsilon = +$ in the case $\mathrm{I}^{\epsilon}_{n\sim n}$(b) which proves the result.

Cases $\mathrm{U}^{\epsilon}_{n,m,l}$(a) and $\mathrm{U}^{\epsilon}_{n\sim n,l}$(a): here $v(c)$ is even by the semistability criterion (Theorem 2.12), $v(\delta_1) = l, v(\delta_2) = n$ and $v(\delta_3) = m$. By definition $\epsilon = +$ if and only if $c \in K^{\times 2}$ (see Definition 2.13). □

9.2 | The value of $E_{C/K}$

We now turn to the value of $E_{C/K}$ and show that $\lambda_{C/K}w_{C/K} = E_{C/K}$ in all cases of Theorem 9.1.

For convenience, we first recall some basic properties of Hilbert symbols. Recall that $(A,B) = 1$ if A or B is a square and whenever A, B are both units for odd places.

Lemma 9.8. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p, and $A, B, C \in K^{\times}$. Then*

(1) $(A+B, -AB) = (A,B)$, *whenever* $A + B \in K^{\times}$.
(2) $(A, -BC) = (\pi_K^{v(B)/2}, -BC)$, *whenever* $A^2 = B + C$ *with* $v(B)$ *and* $v(C)$ *even, and with* $v(B) \leqslant v(C)$ *(equivalently* $v(B) \leqslant v(A^2)$*). If, moreover,* $4|v(B)$ *or* $2|v(A)$, *then* $(A, -BC) = 1$.

Proof.

(1) By [30, Ch. 3 Prop. 2(ii)], $(x, 1-x) = (x, -x) = 1$, whenever $x, 1-x \in K^{\times}$. Using this, we have $(A+B, -AB) = (A+B, -\frac{A}{B}) = (1+\frac{A}{B}, -\frac{A}{B})(B, -\frac{A}{B}) = 1 \times (B, -AB) = (B, A)$.

(2) If $v(A^2) > v(B) = v(C)$, then $B \equiv -C \bmod \pi_K^{2v(A)}$ hence $-BC$ is a square. If $v(C) \geqslant v(B) = v(A^2)$, then $(A, -BC) = (\pi_K^{v(A)}, -BC) = (\pi_K^{v(B)/2}, -BC)$.

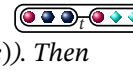
The second statement is then clear as either $\pi_K^{v(\frac{B}{2})}$ is a square, or both A and $-BC$ have even valuation. □

We will also make extensive use of the following identities in conjunction with Lemma 9.8(2).

Lemma 9.9. *Let K be a field and C/K a centred C2D4 curve with $\ell_1 \neq 0$. Then*

(1) $(\frac{1}{2}(\delta_2 + \delta_3))^2 = \delta_2\delta_3 + \ell_1^2 z^2$, *where* $z = \frac{(\alpha_2-\beta_2-\alpha_3+\beta_3)(\alpha_2-\beta_2+\alpha_3-\beta_3)}{2\ell_1} \in K$,
(2) $\eta_1^2 = 4\Delta^2\hat{\delta}_1 + \delta_2\delta_3$,
(3) $\xi^2 = \hat{\delta}_2\hat{\delta}_3 + \delta_1(\frac{\xi_p-\xi_m}{\alpha_1})^2$, *where* $\frac{\xi_p-\xi_m}{\alpha_1} \in K$, $\xi_p = 2(\alpha_2+\alpha_1)(\beta_2+\alpha_1)(\alpha_3+\alpha_1)(\beta_3+\alpha_1)$ *and* $\xi_m = 2(\alpha_2-\alpha_1)(\beta_2-\alpha_1)(\alpha_3-\alpha_1)(\beta_3-\alpha_1)$,
(4) (a) $\eta_2^2 = \hat{\delta}_3 + \delta_2(\alpha_2+\beta_2)^2$,
(b) $\eta_3^2 = \hat{\delta}_2 + \delta_3(\alpha_3+\beta_3)^2$,
(5) $(\delta_2\eta_2 + \delta_3\eta_3)^2 = 4\eta_2\eta_3\delta_2\delta_3 + \ell_1^2(\frac{\delta_2\eta_2-\delta_3\eta_3}{\ell_1})^2$, *where* $\frac{\delta_2\eta_2-\delta_3\eta_3}{\ell_1} \in K$
(6) $(\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2)^2 = 4\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3 + \ell_1^2(\frac{\hat{\delta}_2\eta_3-\hat{\delta}_3\eta_2}{\ell_1})^2$, *where* $\frac{\hat{\delta}_2\eta_3-\hat{\delta}_3\eta_2}{\ell_1} \in K$.
(7) $-\frac{\Delta\ell_1}{c} = \Delta^2\hat{\delta}_1 + \ell_1^2\delta_1 - (\alpha_2\beta_2 - \alpha_3\beta_3)^2$.

Proof. Follows from direct computations using Definition 1.12. □

Lemma 9.10. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \eta_1, \Delta \neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(cases 2(a, d)),*  *(cases 2(b, e)),*  *(cases 2(c, f)),*  *(case $1\times_t 1(a)$),*  *(case $1\tilde{\times}_t 1(a)$),*  *(cases $1\times_t 1(b, c)$) or*  *(cases $1\tilde{\times}_t 1(b, c)$). Then*

$$E_{C/K} = \begin{cases} (\hat{\delta}_1, -\frac{\ell_1}{\Delta}) & \text{cases } 2(a,b,d,e), \\ (\hat{\delta}_1, -c\frac{\ell_1}{\Delta}) & \text{cases } 2(c,f), \\ (c, \delta_1)(\hat{\delta}_1, -\frac{\ell_1}{\Delta}) & \text{cases } 1\times_t 1(a,b,c), 1\tilde{\times}_t 1(a,b,c). \end{cases}$$

Proof. We will abbreviate cases $1\times_t 1$(a,b,c) as 1abc, $1\tilde{\times}_t 1$(a,b,c) as $\tilde{1}$abc and 2(a,b,c) as 2abc. We set $k = t$ for these cases, as the two parameters will play an identical role. We also set $k = 0$ for the cases 2(a,d).

From the cluster picture of C, we find that

- in cases 2abde $v(\delta_2) = v(\delta_3) = v(\hat{\delta}_2) = v(\hat{\delta}_3) = 2k$, $v(\Delta^2\hat{\delta}_1) = 4k$, $v(\xi) \geqslant 2k$, $v(\eta_2), v(\eta_3) \geqslant k$,
- in cases 2cf $v(\delta_2) = 0$, $v(\delta_3) = 2k$, $v(\hat{\delta}_2) = 4k$, $v(\hat{\delta}_3) = 2k$, $v(\Delta^2\hat{\delta}_1) = 2k$, $v(\xi) \geqslant 3k$, $v(\eta_1) \geqslant k$, $v(\eta_2) = 0$, $v(\eta_3) \geqslant 2k$,
- in cases 1a, $\tilde{1}$a $v(\delta_2) = v(\delta_3) = v(\hat{\delta}_2) = v(\hat{\delta}_3) = 2k$, $v(\delta_1) = v(\Delta^2\hat{\delta}_1) = 0$, $v(\xi) \geqslant 2k$, $v(\eta_2), v(\eta_3) \geqslant k$,

By Theorem 2.12(3), $v(c) \equiv k \bmod 2$.

The result follows by combining the following (see below for proof of †). We write 'both even' to mean $(A, B) = 1$ because $v(A)$ and $v(B)$ are even.

- $(\frac{1}{2}(\delta_2+\delta_3), -\ell_1^2\delta_2\delta_3)=1$ (both even for 2cf; 9.9(1) and 9.8(2) for all others),
- $(2, \delta_2\delta_3) = 1$ (both even),

† $(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\delta_2\delta_3\eta_2\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2, -\ell_1^2\hat\delta_2\hat\delta_3\eta_2\eta_3)(\eta_2\eta_3, -\delta_2\delta_3\hat\delta_2\hat\delta_3)$
$$=\begin{cases}1 & \text{cases 2cf}\\ (\pi_K^k, \delta_2\delta_3\hat\delta_2\hat\delta_3) & \text{all other cases}\end{cases},$$

- $(\hat\delta_2\hat\delta_3, -2) = 1$ (both even),
- $(\xi, -\delta_1\hat\delta_2\hat\delta_3) = \begin{cases}(\pi_K^{3k}, -\delta_1\hat\delta_2\hat\delta_3) & \text{cases 2cf}\\ 1 & \text{all other cases}\end{cases}$ (9.9(3) and 9.8(2)),
- $(\eta_1, -\Delta^2\hat\delta_1\delta_2\delta_3) = \begin{cases}(\pi_K^k, -\Delta^2\hat\delta_1\delta_2\delta_3) & \text{cases 2cf}\\ 1 & \text{all other cases}\end{cases}$ (9.9(2) and 9.8(2)),
- $(\ell_1^2, -\ell_2\ell_3) = 1$ (if $\ell_1 \notin K$, then Galois swaps ℓ_2 and ℓ_3, so $v(\ell_1^2), v(\ell_2\ell_3) \in 2\mathbb{Z}$),
- $(c, \Delta^2\hat\delta_1\hat\delta_2\hat\delta_3\delta_1\delta_2\delta_3)=(\pi_K^k, \Delta^2\hat\delta_1\hat\delta_2\hat\delta_3\delta_1\delta_2\delta_3)$ for 2cf $(v(c) \equiv k \bmod 2, v(\Delta^2\hat\delta_1\hat\delta_2\hat\delta_3\delta_1\delta_2\delta_3) \in 2\mathbb{Z})$,
- $(c, \Delta^2) = 1$ for 2cf $(\Delta \in K)$,
- $(c, \hat\delta_2\hat\delta_3\delta_2\delta_3) = (\pi_K^k, \hat\delta_2\hat\delta_3\delta_2\delta_3)$ for 2abde, 1abc, $\tilde{1}$abc $(v(c) \equiv k \bmod 2, v(\hat\delta_2\hat\delta_3\delta_2\delta_3) \in 2\mathbb{Z})$,
- $(c, \delta_1) = 1$ for cases 2abde (both even for 2ad; $\delta_1 \in K^{\times 2}$ for 2be).

□

Proof of †. If Galois does not swap sapphire roots with turquoise roots, then $\ell_1, \delta_2, \delta_3, \hat\delta_2, \hat\delta_3, \eta_2, \eta_3 \in K$, and the claim follows from:

- $(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\delta_2\delta_3\eta_2\eta_3) = (\delta_2\eta_2, \delta_3\eta_3)$ (9.8(1), $\ell_1^2 \in K^{\times 2}$),
- $(\hat\delta_2\eta_3+\hat\delta_3\eta_2, -\ell_1^2\hat\delta_2\hat\delta_3\eta_2\eta_3) = (\hat\delta_2\eta_3, \hat\delta_3\eta_2)$ (9.8(1), $\ell_1^2 \in K^{\times 2}$),
- $(\eta_2, -\delta_2\hat\delta_3) = \begin{cases}1 & \text{cases 2cf}\\ (\pi_K^k, -\delta_2\hat\delta_3) & \text{all other cases}\end{cases}$ (both even for 2cf; 9.9(4a) and 9.8(2) for all others),
- $(\eta_3, -\delta_3\hat\delta_2) = \begin{cases}1 & \text{cases 2cf}\\ (\pi_K^k, -\delta_3\hat\delta_2) & \text{all other cases}\end{cases}$ (9.9(4b) and 9.8(2)),
- $(\delta_2, \delta_3) = 1$ (both even),
- $(\hat\delta_2, \hat\delta_3) = 1$ (both even),

If Galois does swap the sapphire roots with the turquoise roots, then we are not in cases 2cf; moreover, $v(\eta_2) = v(\eta_3) = n$, say, as η_2 and η_3 are Galois conjugate. Recall that $n \geqslant k$ in all these cases, and note that if $n \neq k$, then $\frac{1}{\pi_K^{2k}}\hat\delta_3 \equiv -\frac{1}{\pi_K^{2k}}\delta_2(\alpha_2+\beta_2)^2$ and $\frac{1}{\pi_K^{2k}}\hat\delta_2 \equiv -\frac{1}{\pi_K^{2k}}\delta_3(\alpha_3+\beta_3)^2$ in the residue field by Lemma 9.9(4), so that $\delta_2\delta_3\hat\delta_2\hat\delta_3 \in K^{\times 2}$. The result follows from:

- $(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\delta_2\delta_3\eta_2\eta_3) = (\pi_K^n, -\ell_1^2\delta_2\delta_3\eta_2\eta_3)$ (9.9(7) and 9.8(2)),
- $(\hat\delta_2\eta_3+\hat\delta_3\eta_2, -\ell_1^2\hat\delta_2\hat\delta_3\eta_2\eta_3) = (\pi_K^n, -\ell_1^2\hat\delta_2\hat\delta_3\eta_2\eta_3)$ (9.9(6) and 9.8(2)),
- $(\eta_2\eta_3, -\delta_2\delta_3\hat\delta_2\hat\delta_3) = 1$ (both even),
- $(\pi_K^n, \hat\delta_2\hat\delta_3\delta_2\delta_3) = (\pi_K^k, \hat\delta_2\hat\delta_3\delta_2\delta_3)$ (either $n = k$ or $\hat\delta_2\hat\delta_3\delta_2\delta_3 = \square$).

□

Lemma 9.11. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \eta_1, \Delta \neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(case $I_n^\epsilon(a)$),*  *(case $1\times_t I_n^\epsilon(a)$),*  *(case $I_n^\epsilon(b)$),*  *(case*

$I^{\epsilon}_{2n}(c))$ *or*  *(case* $I^{\epsilon}_{2n}(d)$*). Suppose moreover that* $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$*. Then*

$$E_{C/K} = \begin{cases} (\delta_1, c\xi) & \text{cases } 1^{\pm}_n(a), 1\times_t \mathrm{I}^{\pm}_n(a), \\ (\delta_2, c\eta_1\eta_2) & \text{cases } 1^{\pm}_n(b), \\ (\hat{\delta}_1, -\frac{\ell_1}{\Delta}\eta_1) & \text{cases } 1^{\pm}_{2n}(c), \\ (\hat{\delta}_3, -2c\xi\hat{\delta}_2\eta_2) & \text{cases } 1^{\pm}_{2n}(d). \end{cases}$$

Proof. Note that if Galois does not swap sapphire and turquoise roots, then necessarily ℓ_1, Δ, δ_2, δ_3, $\hat{\delta}_2$, $\hat{\delta}_3$, η_2, $\eta_3 \in K$. From the cluster picture of C, we read off the following basic properties depending on the case:

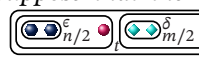
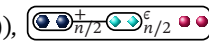
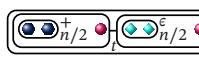
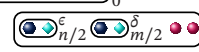
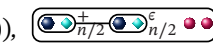
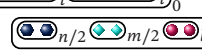
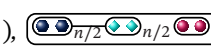
- $1^{\pm}_n$(a): $v(\delta_1) = n, v(\Delta^2\hat{\delta}_1) = v(\delta_2) = v(\delta_3) = v(\hat{\delta}_2) = v(\hat{\delta}_3) = v(\xi) = 0,\ v(c) \equiv 0 \bmod 2$ (Theorem 2.12(3)),
- $1^{\pm}_n$(b): $v(\delta_2) = n, v(\Delta^2\hat{\delta}_1) = v(\delta_1) = v(\delta_3) = v(\hat{\delta}_2) = v(\hat{\delta}_3) = v(\eta_1) = 0, v(c) \equiv 0 \bmod 2$ (Theorem 2.12(3)), $\ell_1, \Delta, \delta_2, \delta_3, \hat{\delta}_2, \hat{\delta}_3, \eta_2, \eta_3 \in K$, $\hat{\delta}_1 \in K^{\times 2}$,
- $1^{\pm}_n$(c): $v(\Delta^2\hat{\delta}_1) = n, v(\delta_1) = v(\delta_2) = v(\delta_3) = v(\hat{\delta}_2) = v(\hat{\delta}_3) = v(\eta_1) = 0, v(\Delta) = v(c) \equiv 0 \bmod 2$ (Theorem 2.12(3) and Lemma 8.6(1)),
- $1^{\pm}_n$(d): $v(\hat{\delta}_3) = n, v(\Delta^2\hat{\delta}_1) = v(\delta_1) = v(\delta_2) = v(\delta_3) = v(\hat{\delta}_2) = v(\xi) = 0,\ v(\Delta) = v(c) \equiv 0 \bmod 2$ (Theorem 2.12(3) and Lemma 8.6(1)), $\ell_1, \Delta, \delta_2, \delta_3, \hat{\delta}_2, \hat{\delta}_3, \eta_2, \eta_3 \in K$,
- $1\times_t \mathrm{I}^{\pm}_n$(a): $v(\delta_1) = 2t+n,\ v(\delta_2) = v(\hat{\delta}_2) = 0,\ v(\delta_3) = v(\Delta^2\hat{\delta}_1) = v(\hat{\delta}_3) = 2t,\ v(\xi) = t,\ v(\Delta) = v(c) \equiv t \bmod 2$ (Theorem 2.12(3) and Lemma 8.6(1)), $\Delta^2 \in K^{\times 2}$.

Recall also that, by hypothesis, $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$ in all cases.

We now simplify the Hilbert symbols in the expression for $E_{C/K}$ according to the case, as shown below. These are obtained simply by cancelling expressions of the form (A, B) where both A and B have even valuation or where A is a perfect square, or by using the identities of Lemma 9.9 together with the Hilbert symbol result for expressions of the form $A^2 = B + C$ of Lemma 9.8(2) as indicated in the final column (the letters in brackets refer to the cases, with 'e' referring to $1\times\mathrm{I}^{\pm}_n(a)$). The proof of the entry $(*)$ is given below. The result follows by taking the product of the Hilbert symbols.

Symbol	$1^{\pm}_n(a)$	$1^{\pm}_n(b)$	$1^{\pm}_{2n}(c)$	$1^{\pm}_{2n}(d)$	$1\times_t \mathrm{I}^{\pm}_n(a)$	Proof
$(\frac{1}{2}(\delta_2+\delta_3), -\ell_1^2\delta_2\delta_3)$	1	$(\frac{1}{2}\delta_3, \delta_2)$	1	1	1	9.9(1), 9.8(2)[*acd*]
$(2, -\ell_1^2\delta_2\delta_3)$	1	$(2, \delta_2)$	1	1	1	
$(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)$	1	$(\delta_3\eta_3, \delta_2)$	1	1	1	9.9(7), 9.8(2)[*acd*]
$(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, -\ell_1^2\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3)$	1	1	1	$(\delta_2\eta_3, \hat{\delta}_3)$	1	9.9(6), 9.8(2)[*abc*]
$(\xi, -\delta_1\delta_2\hat{\delta}_3)$	(ξ, δ_1)	1	1	$(\xi, \hat{\delta}_3)$	$(\xi, \delta_1)(\pi_K^t, -\delta_2\hat{\delta}_3)$	9.9(3), 9.8(2)[*bc*]
$(\eta_2\eta_3, \delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	1	$(\eta_2\eta_3, \delta_2)$	1	$(\eta_2\eta_3, \hat{\delta}_3)$	1	
$(c, \delta_1\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	(c, δ_1)	(c, δ_2)	1	$(c, \hat{\delta}_3)$	$(c, \delta_1)(\pi_K^t, \delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	
$(\eta_1, -\Delta^2\hat{\delta}_1\delta_2\delta_3)$	1	(η_1, δ_2)	$(\eta_1, \hat{\delta}_1)$	1	$(\pi_K^t, -\hat{\delta}_1\delta_2\delta_3)$	9.9(2), 9.8(2)[*ade*]
$(\hat{\delta}_1, -\ell_1/\Delta)$	1 $(*)$	1	$(\hat{\delta}_1, -\ell_1/\Delta)$	1	$(\pi_K^t, \hat{\delta}_1)$	
$(\ell_1^2, -\ell_2\ell_3)$	1	1	1	1	1	
$(2, -\ell_1^2)$	1	1	1	1	1	
$(-2, \hat{\delta}_2\hat{\delta}_3)$	1	1	1	$(-2, \hat{\delta}_3)$	1	

Proof of (∗): In case $1_n^{\pm}$(a), $v(\Delta^2\hat\delta_1) = v(\ell_1) = 0$, so if $v(\Delta) = 0$, then clearly $(\hat\delta_1, -\ell_1/\Delta) = 1$. Suppose $v(\Delta) > 0$ with $v(\Delta/c) > 0$. By Lemma 9.9(7), $\Delta^2\hat\delta_1 \equiv (\alpha_2\beta_2 - \alpha_3\beta_3)^2$ in the residue field. As $\frac{\alpha_2\beta_2-\alpha_3\beta_3}{\ell_1}$ is fixed by Galois, it is K-rational. Thus, $\frac{\Delta^2}{\ell_1^2}\hat\delta_1 \in K^{\times 2}$, and, as $\Delta/\ell_1 \in K$, also $\hat\delta_1 \in K^{\times 2}$. If $v(\Delta) > 0$ with $v(\Delta/c) = 0$, then $v(\Delta) = -v(c)$. By the semistability criterion (Theorem 2.12), $v(c)$ is even. Thus, $v(\Delta)$ is even and $(\hat\delta_1, -\ell_1/\Delta) = 1$. □

Lemma 9.12. *Let $K/\mathbb{Q}_p$ be a finite extension for an odd prime p and C/K a centred semistable C2D4 curve with $\mathcal{P}, \eta_1, \Delta \neq 0$. Suppose that the cluster picture with Frobenius action of C is*  *(case $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$),*  *(case $\mathrm{I}^{\epsilon}_{n} \times_t \mathrm{I}^{\delta}_{m}(a)$),*  *(case $\mathrm{I}^{\epsilon}_{n\sim n}(a)$),*  *($\mathrm{I}^{\epsilon}_{n}\tilde\times_t \mathrm{I}_n(a)$),*  *(case $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$),*  *(case $\mathrm{I}^{\epsilon}_{n\sim n}(b)$),*  *(case $\mathrm{U}^{\epsilon}_{n,m,l}(a)$,),*  *(case $\mathrm{U}^{\epsilon}_{n\sim n,l}(a)$). Moreover, suppose that*

- *in cases $\mathrm{I}^{\epsilon,\delta}_{n,m}(a)$ and $\mathrm{I}^{\epsilon}_{n\sim n}(a)$, $v(\ell_1) = v(\ell_2) = v(\ell_3) = 0$,*
- *in cases $\mathrm{I}^{\epsilon,\delta}_{n,m}(b)$ and $\mathrm{I}^{\epsilon}_{n\sim n}(b)$, $v(\ell_2) = v(\ell_3) = v(\eta_2) = v(\eta_3) = 0$, $v(\ell_1) = \frac{n}{2}$.*

Then

$$E_{C/K} = \begin{cases} (\delta_2, 2c\eta_2)(\delta_3, 2c\eta_3) & \text{case } \mathrm{I}^{\epsilon,\delta}_{n,m}(a), \\ (\delta_2, 2c\eta_2)(\delta_3, 2c\eta_3) & \text{case } \mathrm{I}^{\epsilon}_{n} \times_t \mathrm{I}^{\delta}_{m}(a), \\ (\pi_K^r, \hat\delta_1)(\pi_K^n, \eta_2\eta_3) & \text{case } \mathrm{I}^{\epsilon}_{n\sim n}(a), \\ (\pi_K^n, \eta_2\eta_3) & \text{case } \mathrm{I}^{\epsilon}_{n}\tilde\times_t \mathrm{I}_n(a), \\ (\pi_K^n, -2\eta_1(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2))(\hat\delta_1, \frac{\ell_1}{\Delta}) & \text{case } \mathrm{I}^{\epsilon,\delta}_{n,m}(b), \\ (\pi_K^n, -2\eta_1(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2))(\hat\delta_1, \frac{\ell_1}{\Delta}) & \text{case } \mathrm{I}^{\epsilon}_{n\sim n}(b), \\ (\delta_1\delta_2\delta_3, c) & \text{case } \mathrm{U}^{\epsilon}_{n,m,l}(a), \\ (\delta_1, c) & \text{case } \mathrm{U}^{\epsilon}_{n\sim n,l}(a). \end{cases}$$

Proof. We first record basic properties of the quantities appearing in the Hilbert symbols in the statement. These follow directly from the definitions and the cluster picture of C, along with the semistability criterion (Theorem 2.12) to control the parity of $v(c)$ and occasionally Hensel's lemma to show that certain quantities are squares in K when they are squares over the residue field.

We then simplify the Hilbert symbols defining $E_{C/K}$ according to the cluster picture of C. Here we cancel expressions of the form (A, B) where both A and B have even valuation or where A is a perfect square, and occasionally use the identity $(A + B, -AB) = (A, B)$ (Lemma 9.8(1), indicated by a ∗) or the Hilbert symbol expression of Lemma 9.8(2) together with the appropriate identity from Lemma 9.9 (indicated by a †). The simplified expressions are displayed in the tables below. The result follows by taking the product of the Hilbert symbols.

$\mathrm{I}^{\epsilon,\delta}_{n,m}$(a): $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\delta_1) = v(\Delta^2\hat\delta_1) = v(\hat\delta_2) = v(\hat\delta_3) = v(\eta_2) = v(\eta_3) = 0$, $v(\xi) \geqslant 0$, $v(c) \equiv 0 \bmod 2$, $\ell_1, \Delta, \delta_2, \delta_3, \eta_2, \eta_3 \in K^\times$, $\eta_1 = 2\square$, $\hat\delta_1 = \square$;

$\mathrm{I}^{\epsilon}_{n}\times_t \mathrm{I}^{\delta}_{m}$(a): $v(\Delta^2\hat\delta_1) = 0$, $v(\hat\delta_2) = v(\hat\delta_3) = 2t$, $v(\xi) \geqslant 2t$, $\ell_1, \Delta, \delta_2, \delta_3, \hat\delta_2, \hat\delta_3, \eta_2, \eta_3 \in K^\times$, $\delta_1 = \square$, $\eta_1 = 2\square$, $\hat\delta_1 = \square$, $\hat\delta_2 = \square$, $\hat\delta_3 = \square$;

$\mathrm{I}^{\epsilon}_{n\sim n}$(a): $v(\ell_1) = v(\ell_2) = v(\ell_3) = v(\delta_1) = v(\Delta^2\hat\delta_1) = v(\hat\delta_2) = v(\hat\delta_3) = v(\eta_1) = v(\eta_2) = v(\eta_3) = 0$, $v(\delta_2) = v(\delta_3) = n$, $v(\xi) \geqslant 0$, $v(c) \equiv 0 \bmod 2$, $v(\Delta) = v(c) + r \equiv r \bmod 2$;

$\mathrm{I}_n^\epsilon \tilde{\times}_t \mathrm{I}_n(\mathrm{a})$: $v(\ell_1)=v(\ell_2)=v(\ell_3)=v(\delta_1)=v(\Delta^2\hat{\delta}_1)=v(\eta_1)=0$, $v(\hat{\delta}_2)=v(\hat{\delta}_3)=2t$, $v(\eta_2)=v(\eta_3)=t$, $v(\delta_2)=v(\delta_3)=n+2t$, $v(\xi)\geqslant 2t$, $v(\Delta)=v(c)\equiv t \bmod 2$ (Theorem 2.12(3), Lemma 8.6), $\hat{\delta}_1=\delta_1\square$ (as $v(\delta_1)=0$, $\delta_1\neq\square$ and, by Lemma 9.3 $v(\hat{\delta}_1)\in 2\mathbb{Z}$, $\hat{\delta}_1\neq\square$).

Symbol	$\mathrm{I}_{n,m}^{\epsilon,\delta}(\mathrm{a}), \mathrm{I}_n^\epsilon \times_t \mathrm{I}_m^\delta(\mathrm{a})$	$\mathrm{I}_{n\sim n}^\epsilon(\mathrm{a})$	$\mathrm{I}_n^\epsilon \tilde{\times}_t \mathrm{I}_n(\mathrm{a})$
$(\frac{1}{2}(\delta_2+\delta_3), -\ell_1^2\delta_2\delta_3)$	$(\delta_2,\delta_3)(2,\delta_2\delta_3)$ *	$(\pi_K^n, -\ell_1^2\delta_2\delta_3)$ †	$(\pi_K^n, -\ell_1^2\delta_2\delta_3)$ †
$(2, -\ell_1^2\delta_2\delta_3)$	$(2,\delta_2\delta_3)$	1	1
$(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)$	$(\delta_2\eta_2,\delta_3\eta_3)$ *	$(\pi_K^n, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)$ †	$(\pi_K^{n+t}, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)$ †
$(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, -\ell_1^2\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3)$	(η_2,η_3) *	1 †	$(\pi_K^t, -\ell_1^2\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3)$ †
$(\xi, -\delta_1\hat{\delta}_2\hat{\delta}_3)$	1 †	1 †	1 †
$(\eta_2\eta_3, \delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	$(\eta_2\eta_3,\delta_2\delta_3)$	1	1
$(c, \delta_1\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	$(c,\delta_2\delta_3)$	1	$(\pi_K^t, \delta_1\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$
$(\eta_1, -\Delta^2\hat{\delta}_1\delta_2\delta_3)$	$(2,\delta_2\delta_3)$	1	1
$(\hat{\delta}_1, -\ell_1/\Delta)$	1	$(\hat{\delta}_1, \pi_K^r)$	(δ_1, π_K^t)
$(\ell_1^2, -\ell_2\ell_3)$	1	1	1
$(2, -\ell_1^2)$	1	1	1
$(-2, \hat{\delta}_2\hat{\delta}_3)$	1	1	1

$\mathrm{I}_{n,m}^{\epsilon,\delta}$(b): $v(\ell_2)=v(\ell_3)=v(\eta_2)=v(\eta_3)=v(\delta_1)=v(\delta_2)=v(\delta_3)=v(\hat{\delta}_2)=v(\hat{\delta}_3)=v(\eta_1)=0$, $v(\ell_1)=\frac{n}{2}$, $v(\xi)\geqslant 0$, $v(c)\equiv 0 \bmod 2$, $v(\Delta^2)=n+2r+2v(c)\equiv n \bmod 2$, $\ell_2\ell_3=\square$, $\eta_1=-\square$, $v(\delta_2+\delta_3)=v(\delta_2\eta_2+\delta_3\eta_3)=v(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2)=0$ (because $\delta_2\equiv\delta_3$, $\eta_2\equiv\eta_3$, $\hat{\delta}_2\equiv\hat{\delta}_3$ in the residue field);

$\mathrm{I}_{n\sim n}^\epsilon$(b): $v(\ell_2)=v(\ell_3)=v(\eta_2)=v(\eta_3)=v(\delta_1)=v(\delta_2)=v(\delta_3)=v(\hat{\delta}_2)=v(\hat{\delta}_3)=v(\eta_1)=0$, $v(\ell_1)=\frac{n}{2}$, $v(\hat{\delta}_1\Delta^2)=n$, $v(\xi)\geqslant 0$, $v(c)\equiv 0 \bmod 2$, $v(\hat{\delta}_1)\equiv v(\hat{\delta}_1\Delta^2)-v(\Delta^2/c^2)\equiv 0 \bmod 2$, $\ell_2\ell_3=\square$, $v(\delta_2+\delta_3)=v(\delta_2\eta_2+\delta_3\eta_3)=v(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2)=0$ (because $\delta_2\equiv\delta_3$, $\eta_2\equiv\eta_3$, $\hat{\delta}_2\equiv\hat{\delta}_3$ in the residue field);

$\mathrm{U}_{n,m,l}^\epsilon$(a): $v(\ell_1)=v(\ell_2)=v(\ell_3)=v(\hat{\delta}_1\Delta^2)=v(\hat{\delta}_2)=v(\hat{\delta}_3)=v(\eta_1)=v(\eta_2)=v(\eta_3)=v(\xi)=0$, $v(\Delta)\equiv v(c)\equiv 0 \bmod 2$ (Theorem 2.12(3), Lemma 8.6), $v(\hat{\delta}_1)\equiv 0 \bmod 2$, $\delta_2,\delta_3,\eta_2,\eta_3\in K$, $\eta_1,\eta_2,\eta_3=2\square$;

$\mathrm{U}_{n\sim n,l}^\epsilon$(a): $v(\ell_1)=v(\ell_2)=v(\ell_3)=v(\hat{\delta}_1\Delta^2)=v(\hat{\delta}_2)=v(\hat{\delta}_3)=v(\eta_1)=v(\eta_2)=v(\eta_3)=v(\xi)=0$, $v(\delta_2)=v(\delta_3)=n$, $v(\Delta)\equiv v(c)\equiv 0 \bmod 2$ (Theorem 2.12(3), Lemma 8.6), $v(\hat{\delta}_1)\equiv 0 \bmod 2\eta_2\eta_3=\square$.

Symbol	$\mathrm{I}_{n,m}^{\epsilon,\delta}(\mathrm{b})$	$\mathrm{I}_{n\sim n}^\epsilon(\mathrm{b})$	$\mathrm{U}_{n,m,l}^\epsilon(\mathrm{a})$	$\mathrm{U}_{n\sim n,l}^\epsilon(\mathrm{a})$
$(\frac{1}{2}(\delta_2+\delta_3), -\ell_1^2\delta_2\delta_3)$	$(2(\delta_2+\delta_3), \pi_K^n)$	$(2(\delta_2+\delta_3), \pi_K^n)$	$(\delta_2,\delta_3)(2,-\ell_1^2\delta_2\delta_3)$ *	$(\pi_K^n, -\ell_1^2\delta_2\delta_3)$ †
$(2, -\ell_1^2\delta_2\delta_3)$	$(2,\ell_1^2)$	$(2,\ell_1^2)$	$(2,-\ell_1^2\delta_2\delta_3)$	1
$(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)$	$(\delta_2\eta_2+\delta_3\eta_3, \pi_K^n)$	$(\delta_2\eta_2+\delta_3\eta_3, \pi_K^n)$	$(2\delta_2, 2\delta_3)$ *	$(\pi_K^n, -\ell_1^2\delta_2\delta_3)$ †
$(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, -\ell_1^2\eta_2\eta_3\hat{\delta}_2\hat{\delta}_3)$	$(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, \pi_K^n)$	$(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, \pi_K^n)$	1 †	1 †
$(\xi, -\delta_1\hat{\delta}_2\hat{\delta}_3)$	1 †	1 †	1 †	1 †
$(\eta_2\eta_3, \delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	1	1	1	1
$(c, \delta_1\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3)$	1	1	$(c, \delta_1\delta_2\delta_3)$	(c, δ_1)
$(\eta_1, -\Delta^2\hat{\delta}_1\delta_2\delta_3)$	$(\eta_1, \pi_K^n)(\hat{\delta}_1, -1)$	(η_1, π_K^n)	$(2, \delta_2\delta_3)$	1
$(\hat{\delta}_1, -\ell_1/\Delta)$	$(\hat{\delta}_1, -\ell_1/\Delta)$	$(\hat{\delta}_1, \ell_1/\Delta)$	1	1
$(\ell_1^2, -\ell_2\ell_3)$	$(\pi_K^n, -1)$	$(\pi_K^n, -1)$	1	1
$(2, -\ell_1^2)$	$(2,\ell_1^2)$	$(2,\ell_1^2)$	1	1
$(-2, \hat{\delta}_2\hat{\delta}_3)$	1	1	1	1

□

10 | EVEN PLACES

In this section, we look at C2D4 curves with good ordinary reduction over 2-adic fields. Such curves admit a nice model — essentially, curves with good ordinary reduction turn out to be those with cluster picture  with depth of each twin precisely $v(4)$. Theorem 10.3 then shows that Conjecture 1.14 holds for curves with this model and a specific Richelot isogeny. In the next section, we will show that the conjecture is independent of the choice of model and independent of the choice of the isogeny, and hence, that it holds for all curves with good ordinary reduction at 2-adic primes.

We begin with a preliminary lemma about 2-adic fields and Hilbert symbols.

Lemma 10.1. *Let $K/\mathbb{Q}_2$ be a finite extension. Then*

(i) *$K(\sqrt{x})/K$ is unramified if and only if $x = \square \cdot (1+4t)$ for some $t \in \mathcal{O}_K$.*
(ii) *If $x = \square \cdot (1+4t)$ for some $t \in \mathcal{O}_K$, then*

$$(x, u) = 1 \qquad \text{for all } u \in \mathcal{O}_K^\times.$$

(iii) *If $F = K(\sqrt{L})$ is the quadratic unramified extension and $x \in F$ such that $x^2 + \mathrm{Frob}_{F/K}\, x^2$ is a unit, then*

$$(x^2 + \mathrm{Frob}_{F/K}\, x^2, -1) = (2, L).$$

Proof.

(i) Fix a set of representatives $S \supseteq \{0,1\}$ of $\mathcal{O}_K/(\pi_K)$ and consider the equation

$$(a_0 + a_1\pi_K + a_2\pi_K^2 + \cdots)^2 \equiv 1 + 4t \bmod 4\pi_K, \qquad a_i \in S,$$

for a given $t \in \mathcal{O}_K$. Equating the coefficients of powers of π_K, we must necessarily have $a_0 = 1$ and $a_1 = \cdots = a_{n-1} = 0$ for $n = v(2)$. The equation is then soluble if and only if $a_n^2 + a_n \equiv t \bmod \pi_K$ is soluble. Hence, it is always soluble in the quadratic unramified extension of K, but not in K for a suitable choice of t.

It follows that elements of the form $x = \square \cdot (1+4t)$ with $t \in \mathcal{O}_K$ are squares in the quadratic unramified extension of K, and that some of these elements have $K(\sqrt{x}) \neq K$. The set of such elements is a subgroup of $K^\times$ that properly contains $K^{\times 2}$, and hence, must contain all the elements $x \in K$ such that $K(\sqrt{x})/K$ is unramified.

(ii) Follows from (i) and the fact that all units in K are norms from any unramified extension.

(iii) Write $x = a + b\sqrt{L}$ for some $a, b \in K$. Then $x^2 + \mathrm{Frob}_{F/K}\, x^2 = 2a^2 + 2Lb^2$, so that

$$(x^2 + \mathrm{Frob}_{F/K}\, x^2, -L) = (2, -L) = (2, L),$$

as $(a^2 + Lb^2) = (a + b\sqrt{-L})(a - b\sqrt{-L})$ is a norm from $K(\sqrt{-L})$, and $(2,-1) = 1$. Also

$$(x^2 + \mathrm{Frob}_{F/K}\, x^2, L) = 1,$$

because $x^2 + \mathrm{Frob}_{F/K}\, x^2$ is a unit by hypothesis, and hence a norm from the unramified extension $K(\sqrt{L})/K$. The result follows. □

We now turn to models of genus 2 curves with ordinary reduction.

Proposition 10.2. *Let $K/\mathbb{Q}_2$ be a finite extension with residue field k of size $|k| \geqslant 4$, and let C/K be a genus 2 curve with good reduction.*

(i) *C/K has ordinary reduction if and only if it admits a model of the form*

$$y^2 = cf(x)$$

with $c \equiv 1 \bmod 4$, and with $f(x) \in \mathcal{O}_K[x]$ monic whose roots can be labelled α_1, β_1, α_2, β_2, α_3, β_3 so that for all $i \neq j$

$$(x-\alpha_i)(x-\beta_i) \in K^{nr}[x], \quad \upsilon(\alpha_i-\beta_i)=\upsilon(4), \quad \upsilon(\alpha_i-\alpha_j)=\upsilon(\beta_i-\beta_j)=\upsilon(\alpha_i-\beta_j)=0.$$

For this model, the kernel of the reduction map on the 2-torsion points of Jac C/K *consists of 0, $[(\alpha_1,0),(\beta_1,0)]$, $[(\alpha_2,0),(\beta_2,0)]$ and $[(\alpha_3,0),(\beta_3,0)]$.*

(ii) *If C/K has ordinary reduction and ϕ is the Richelot isogeny whose kernel is precisely the 2-torsion points in the kernel of the reduction map, then the Richelot dual curve $\widehat{C}$ also has good ordinary reduction.*

(iii) *If C/K is a C2D4 curve with ordinary reduction, such that the kernel of the associated Richelot isogeny agrees with the kernel of the reduction map on 2-torsion points, and if $|k| \geqslant 32$, then the model in (i) can be further taken to have the C2D4 structure defined by the α_i, β_i and*

$$\frac{\delta_2+\delta_3}{16}, \quad \frac{\delta_2\eta_2+\delta_3\eta_3}{32}, \quad \frac{\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2}{8} \quad \in \quad \mathcal{O}_K^{\times}.$$

Proof. (i) This is [16, Theorem 1.2 and Proposition 1.16].

(ii) Take the model $y^2 = cf(x)$ for C/K given by (i). We will show that $\widehat{C}$ has a similar model, and hence also has good ordinary reduction by (i).

Using the fact that α_i, β_i have non-negative valuations (they satisfy a polynomial with unit leading term and integral coefficients) and the valuations of their pairwise differences, one readily checks that:

- $\upsilon(\ell_1) = \upsilon(\ell_2) = \upsilon(\ell_3) = \upsilon(2)$,
- $\hat{r}(x), \hat{s}(x), \hat{t}(x) \in \mathcal{O}_K^{nr}[x]$, so that $\upsilon(\hat{\alpha}_i), \upsilon(\hat{\beta}_i) \geqslant 0$ (see Definition 2.1),
- $\Delta/c \equiv 2(\alpha_1-\alpha_2)(\alpha_3-\alpha_1)(\alpha_3-\alpha_2) \bmod 4$, so that $\upsilon(\Delta) = \upsilon(2)$.

By Proposition 8.4(1,2,3), we deduce that $\upsilon(\hat{\alpha}_i-\hat{\beta}_i) = 0$ for $i = 1,2,3$, so no cluster of $\widehat{C}$ of size < 6 can contain two roots of the same colour. Also, there cannot be such a cluster that contains roots of all three colours: otherwise, Lemma 8.6(3) would imply that $\upsilon\left(\frac{\Delta(\widehat{C})}{c(\widehat{C})}\right) > 0$, but by Proposition 8.4(7) $\upsilon\left(\frac{\Delta(\widehat{C})}{c(\widehat{C})}\right) = \upsilon\left(\frac{2\Delta(C)/c^2}{\ell_1\ell_2\ell_2/\Delta(C)}\right) = 0$. Thus, the only possible clusters are twins that contain roots of different colours.

By Proposition 8.4(4,5,6),

$$\upsilon(\hat{\alpha}_2-\hat{\alpha}_3) + \upsilon(\hat{\alpha}_2-\hat{\beta}_3) + \upsilon(\hat{\beta}_2-\hat{\alpha}_3) + \upsilon(\hat{\beta}_2-\hat{\beta}_3) = \upsilon(4),$$

and similarly for the indices 1,2 and 1,3. It follows that the cluster picture of $\widehat{C}$ must be  , with the depth of each twin exactly $\upsilon(4)$. Since $r(x), s(x), t(x) \in K^{nr}[x]$, the polynomials $\hat{r}(x), \hat{s}(x), \hat{t}(x)$ also have coefficients in K^{nr}.

To deduce that $\widehat{C}$ has good ordinary reduction using (i), it remains to show that the leading term $c(\widehat{C}) = \frac{\ell_1\ell_2\ell_3}{\Delta}$ is of the form $\square \cdot (1+4z)$ for some $z \in \mathcal{O}_K$. Note that the quadratic twist $\widehat{C}'$

of $\widehat{C}$ by $c(\widehat{C})$ does have good ordinary reduction by (i), and hence, its Jacobian has good reduction. The Jacobian of $\widehat{C}$ also has good reduction, being isogenous to $\operatorname{Jac} C/K$. Thus, $K(\sqrt{c(\widehat{C})})/K$ must be unramified, and hence, $c(\widehat{C})$ is of the required form by Lemma 10.1(i).

(iii) Take the model for C/K given by (i). Relabelling the roots if necessary, by (ii), we may assume that the C2D4 structure is given by the α_i, β_i. We now need to adjust the model so that the claimed invariants are units.

As $v(\alpha_1-\beta_1)\geqslant v(4)$, the term $\frac{\alpha_1+\beta_1}{2}$ lies in $\mathcal{O}_K$. Applying the translation to the x-coordinate $x\mapsto x+\frac{\alpha_1+\beta_1}{2}$, we may thus assume that the C2D4 model is centred, that is, $\alpha_1=-\beta_1$.

Recall from Definition 6.3 that for $t\in K\setminus\{\frac{1}{\alpha_1},-\frac{1}{\alpha_1}\}$, we have a Möbius transformation M_t and model C_t. We now proceed as in the proof of Theorem 6.6 to pick a suitable value for $t\in\mathcal{O}_K$ that gives a model with the required properties.

By construction, the roots $\alpha_i(C_t)=M_t(\alpha_i)$ and $\beta_i(C_t)=M_t(\beta_i)$ for the model C_t satisfy $(x-\alpha_i(C_t))(x-\beta_i(C_t))\in K^{nr}[x]$. As in the first paragraph of the proof of Theorem 6.6, if $t\not\equiv -1/\alpha_i,-1/\beta_i$ in k for any i, then the model C_t will also have $v(\alpha_i(C_t)),v(\beta_i(C_t))\geqslant 0$, $v(\alpha_i(C_t)-\beta_i(C_t))=v(4)$ and $v(r-r')=0$ for all other pairs of roots. As in the last paragraph of the proof of (ii), $c(C_t)$ is necessarily of the form $\square\cdot(1+4z)$ for some $z\in\mathcal{O}_K$. It remains to ensure that $\frac{\delta_2+\delta_3}{16}$, $\frac{\delta_2\eta_2+\delta_3\eta_3}{32}$ and $\frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{8}$ are units for the C_t model.

Write $\alpha_i=\beta_i+4u_i$, so that $v(u_i)=0$. A direct computation shows that

$$\begin{aligned}
\tfrac{\delta_2(C_t)+\delta_3(C_t)}{16} &= \frac{F_1(t)}{(1+\alpha_2t)^2(1+\beta_2t)^2(1+\alpha_3t)^2(1+\beta_3t)^2},\\
\tfrac{\delta_2(C_t)\eta_2(C_t)+\delta_3(C_t)\eta_3(C_t)}{32} &= \frac{F_2(t)}{(1+\alpha_2t)^4(1+\beta_2t)^4(1+\alpha_3t)^4(1+\beta_3t)^4},\\
\tfrac{\hat\delta_2(C_t)\eta_3(C_t)+\hat\delta_3(C_t)\eta_2(C_t)}{8} &= \frac{F_3(t)}{(1+\alpha_2t)^4(1+\beta_2t)^4(1+\alpha_3t)^4(1+\beta_3t)^4},
\end{aligned}$$

where $F_1(t),F_2(t),F_3(t)$ are polynomials in $\mathcal{O}_K[t]$ that reduce in $k[t]$ to

$$\begin{aligned}
F_1(t)\equiv\ & (\beta_3^4u_2^2+\beta_2^4u_3^2)t^4+(u_2^2+u_3^2),\\
F_2(t)\equiv\ & (\beta_2^4\beta_3^8u_2^2+\beta_3^4\beta_2^8u_3^2)t^{10}+(\beta_2^2\beta_3^8u_2^2+\beta_3^2\beta_2^8u_3^2)t^8+\\
&+(\beta_2^4u_2^2+\beta_3^4u_3^2)t^2+(\beta_2^2u_2^2+\beta_3^2u_3^2),\\
F_3(t)\equiv\ & (\beta_2^8\beta_3^6+\beta_3^8\beta_2^6)t^8+(\beta_2^8+\beta_3^8)t^2+(\beta_2^6+\beta_3^6).
\end{aligned}$$

None of these is the zero polynomial in $k(t)$, as we now explain. Since $\beta_2\not\equiv\beta_3$ and $z\mapsto z^2$ is an automorphism of k, we deduce that $\beta_2^2\not\equiv\beta_3^2$, $\beta_2^4\not\equiv\beta_3^4$ and $\beta_2^8\not\equiv\beta_3^8$; this deals with $F_3(t)$. Moreover, if $u_2^2\equiv u_3^2$, then $\beta_3^4u_2^2\not\equiv\beta_2^4u_3^2$, so $F_1(t)$ is not zero. Finally, if $\beta_2^2u_2^2\equiv\beta_3^2u_3^2$, then $\beta_2^2\beta_3^8u_2^2\not\equiv\beta_3^2\beta_2^8u_3^2$, so $F_2(t)$ is not zero.

Thus, so long as $t\in\mathcal{O}_K$ avoids the residues of the $\bar k$-roots of $F_1(t)$, $F_2(t)$ and $F_3(t)$ (at most 22 such) and the residues of $-1/\alpha_i,-1/\beta_i$ (at most 6 such), the required expressions will be units. □

Theorem 10.3. *Let $K/\mathbb{Q}_2$ be a finite extension and C/K a C2D4 curve with good ordinary reduction given by $y^2=cf(x)$ with $f(x)\in\mathcal{O}_K[x]$ monic, satisfying $(x-\alpha_i)(x-\beta_i)\in K^{nr}[x]$ and $v(\alpha_i-\beta_i)=v(4)$ for all i, and $v(r-r')=0$ for all other pairs of roots r,r'. Suppose moreover that $\mathcal{P},\Delta\neq 0$ and that $\frac{\delta_2+\delta_3}{16},\frac{\delta_2\eta_2+\delta_3\eta_3}{32},\frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{8}\in\mathcal{O}_K^\times$. Then Conjecture 1.14 holds for C/K.*

Proof. As $\operatorname{Jac} C/K$ has good reduction, $w_{\operatorname{Jac} C/K}=1$.

By Proposition 10.2(ii), $\widehat{C}/K$ also has good ordinary reduction, so that neither C/K nor $\widehat{C}/K$ are deficient. Since the kernel of the reduction map on 2-torsion points coincides with the kernel of the Richelot isogeny ϕ on $\mathrm{Jac}\, C/K$, Lemma 3.4 and Theorem A.1 show that $\lambda_{C/K,\phi} = 1 \cdot 1 \cdot (-1)^{[K:\mathbb{Q}_2]\cdot 2} = 1$. It remains to prove that the product of Hilbert symbols is also trivial, that is, $E_{C/K} = 1$.

Since α_1, β_1 are integral, $\alpha_1+\beta_1 \in \mathcal{O}_K$ and $4|(\alpha_1-\beta_1)$, it follows that $\frac{\alpha_1+\beta_1}{2} \in \mathcal{O}_K$. The change of variables $x \mapsto x+\frac{\alpha_1+\beta_1}{2}$ does not change any of the hypotheses on C in the statement, including that $f(x) \in \mathcal{O}_K[x]$. We may (and will) therefore assume that C is centred, that is, $\alpha_1 = -\beta_1$.

Let $\gamma_i = \frac{\alpha_i+\beta_i}{2}$, so that $\{\gamma_1, \gamma_2, \gamma_3\}$ is preserved by Galois. Note that $\gamma_i \equiv \alpha_i \equiv \beta_i \bmod 2$, $\gamma_i^2 \equiv \alpha_i^2 \equiv \beta_i^2 \bmod 4$ and $\gamma_i^4 \equiv \alpha_i^4 \equiv \beta_i^4 \bmod 8$. As C is centred, $\gamma_1 \equiv 0 \bmod 2$, and $v(\gamma_2) = v(\gamma_3) = 0$.

Explicit computation shows that

- $\Delta^2\hat{\delta}_1 \equiv (\gamma_2-\gamma_3)^4 \bmod 8$, so that $\Delta^2\hat{\delta}_1 = \square$,
- $\frac{1}{2}\eta_2 \equiv \gamma_2^2 \bmod 4$, $\frac{1}{2}\eta_3 \equiv \gamma_3^2 \bmod 4$, so $\eta_2\eta_3 = \square(1+4z)$,
- $\frac{1}{4}\hat{\delta}_2 \equiv \gamma_3^4 \bmod 8$, $\frac{1}{4}\hat{\delta}_3 \equiv \gamma_2^4 \bmod 8$, so $\hat{\delta}_2\hat{\delta}_3 = \square$,
- $\frac{1}{4}\xi \equiv \gamma_2^2\gamma_3^2 \bmod 4$, so that $\xi = \square(1+4z')$,
- $\frac{1}{2}\eta_1 \equiv (\gamma_2-\gamma_3)^2 \equiv \frac{1}{4}\ell_1^2 \bmod 4$, so that $\eta_1 = 2\ell_1^2\square(1+4z'')$

for some $z, z', z'' \in \mathcal{O}_K$. Moreover,

- $\ell_1^2 = \square(1+4z)$ for some $z \in \mathcal{O}_K$ by Lemma 10.1(i), and
- $\frac{\ell_1\ell_2\ell_3}{\Delta} = \square(1+4z)$ for some $z \in \mathcal{O}_K$ by the final paragraph of the proof of Proposition 10.2(ii).

Recall from Lemma 10.1(ii) that if $a = 1+4z$ for $z \in \mathcal{O}_K$ and $b \in K^\times$ has even valuation, then $(a,b) = 1$. We can thus simplify the Hilbert symbols defining $E_{C/K}$ as follows:

$$\begin{aligned}
(\xi, -\delta_1\hat{\delta}_2\hat{\delta}_3) &= 1,\\
(\eta_2\eta_3, -\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3) &= 1,\\
(c, \delta_1\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3) &= 1,\\
(\hat{\delta}_2\hat{\delta}_3, -2) &= 1,\\
(\eta_1, -\delta_2\delta_3\hat{\delta}_2\hat{\delta}_3) &= (2\ell_1^2, -\delta_2\delta_3) = (2, -\delta_2\delta_3),\\
(\hat{\delta}_1, -\tfrac{\ell_1}{\Delta})(\ell_1^2, -\ell_2\ell_3) &= (\ell_1^2\hat{\delta}_1, -\tfrac{\ell_1}{\Delta})(\ell_1^2, \tfrac{\ell_1\ell_2\ell_3}{\Delta}) = \big(\big(\tfrac{\ell_1}{\Delta}\big)^2\hat{\delta}_1\Delta^2, -\tfrac{\ell_1}{\Delta}\big) = 1.
\end{aligned}$$

Hence,

$$E_{C/K} = (2, \ell_1^2\delta_2\delta_3)(\delta_2+\delta_3, -\ell_1^2\delta_2\delta_3)(\delta_2\eta_2+\delta_3\eta_3, -\ell_1^2\eta_2\eta_3\delta_2\delta_3)(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, -\ell_1^2\hat{\delta}_2\hat{\delta}_3\eta_2\eta_3).$$

Suppose that Frob_K does not swap the sets $\{\alpha_2, \beta_2\}$ and $\{\alpha_3, \beta_3\}$. In particular, $\ell_1 \in K$, so $\ell_1^2 = \square$. Also $\gamma_i, \delta_i, \eta_i, \hat{\delta}_i \in K$, as they are all fixed by Frob_K. By Lemma 9.8(1),

$$\begin{aligned}
(\delta_2+\delta_3, -\delta_2\delta_3) &= (\delta_2, \delta_3),\\
(\delta_2\eta_2+\delta_3\eta_3, -\delta_2\delta_3\eta_2\eta_3) &= (\delta_2\eta_2, \delta_3\eta_3),\\
(\hat{\delta}_2\eta_3+\hat{\delta}_3\eta_2, -\hat{\delta}_2\hat{\delta}_3\eta_2\eta_3) &= (\hat{\delta}_2\eta_2, \hat{\delta}_3\eta_3).
\end{aligned}$$

As $\frac{1}{4}\hat{\delta}_2 \equiv \gamma_3^4 \bmod 8$, we have $\hat{\delta}_2 = \square$, and as $\frac{1}{2}\eta_2 \equiv \gamma_2^2 \bmod 4$, we have $\eta_2 = 2\square(1+4z)$ for some $z \in \mathcal{O}_K$, and similarly, for $\hat{\delta}_3$ and η_3. Thus,

$$E_{C/K} = (2, \delta_2\delta_3)(\delta_2, \delta_3)(\delta_2\eta_2, \delta_3\eta_3)(\eta_2, \eta_3) = (2, \delta_2\delta_3)(\delta_2, \eta_3)(\delta_3, \eta_2)$$
$$= (2, \delta_2\delta_3)(\delta_2, 2)(\delta_3, 2) = 1.$$

Suppose now that Frob_K swaps the sets $\{\alpha_2, \beta_2\}$ and $\{\alpha_3, \beta_3\}$, so that it interchanges $\delta_2 \leftrightarrow \delta_3$, $\eta_2 \leftrightarrow \eta_3$, $\hat\delta_2 \leftrightarrow \hat\delta_3$. Since $\ell_1, (\alpha_2-\beta_2)(\alpha_3-\beta_3) \in K^{nr}$ and all units are norms from quadratic unramified extensions, $(\ell_1^2, u) = (\delta_2\delta_3, u) = 1$ for all $u \in \mathcal{O}_K^\times$. Recall that by hypothesis $\frac{\delta_2+\delta_3}{16}, \frac{\delta_2\eta_2+\delta_3\eta_3}{32}, \frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{8} \in \mathcal{O}_K^\times$, and that $\hat\delta_2\hat\delta_3 = \square$, which simplifies the expression for $E_{C/K}$:

$$E_{C/K} = (2, \ell_1^2\delta_2\delta_3)\left(\frac{\delta_2+\delta_3}{16}, -\ell_1^2\delta_2\delta_3\right)\left(\frac{\delta_2\eta_2+\delta_3\eta_3}{32}, -\delta_2\delta_3\eta_2\eta_3\right)\cdot$$
$$\cdot(2, -\delta_2\delta_3\eta_2\eta_3)\left(\frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{8}, -\eta_2\eta_3\right)(2, -\eta_2\eta_3)$$
$$= (2, \ell_1^2)\left(\frac{\delta_2+\delta_3}{16}\cdot\frac{\delta_2\eta_2+\delta_3\eta_3}{32}\cdot\frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{8}, -1\right).$$

Write $\alpha_2-\beta_2 = 4u_2$ and $\alpha_3-\beta_3 = 4u_3$, so that $v(u_2) = v(u_3) = 0$ and Frob_K interchanges $u_2^2 \leftrightarrow u_3^2$. Then $\frac{1}{16}(\delta_2+\delta_3) = u_2^2+u_3^2$, $\frac{1}{32}(\delta_2\eta_2+\delta_3\eta_3) \equiv u_2^2\gamma_2^2+u_3^2\gamma_3^2 \bmod 4$ and $\frac{1}{8}(\hat\delta_2\eta_3+\hat\delta_3\eta_2) \equiv \gamma_2^6+\gamma_3^6 \bmod 4$, and all three are units. By Lemma 10.1(ii), $(1+4z, -1) = 1$ for all $z \in \mathcal{O}_K$, so

$$E_{C/K} = (2, \ell_1^2)((u_2^2+u_3^2)(u_2^2\gamma_2^2+u_3^2\gamma_3^2)(\gamma_2^6+\gamma_3^6), -1).$$

By Lemma 10.1(iii), $(\gamma_2^6+\gamma_3^6, -1) = (2, \ell_1^2)$, as γ_2^3 lies in the quadratic unramified extension $K(\ell_1)$ of K. If $\mathrm{Frob}_K^2 u_2 = u_2$, then similarly $(u_2^2+u_3^2, -1) = (2, \ell_1^2)$ and $(u_2^2\gamma_2^2+u_3^2\gamma_3^2, -1) = (2, \ell_1^2)$, so that $E_{C/K} = 1$. Otherwise $\mathrm{Frob}_K(u_2u_3(\gamma_2-\gamma_3)) = u_3(-u_2)(\gamma_3-\gamma_2) = u_2u_3(\gamma_2-\gamma_3)$, so that

$$(u_2^2\gamma_2^2+u_3^2\gamma_3^2)(u_2^2+u_3^2) = (u_2^2\gamma_2+u_3^2\gamma_3)^2 + u_2^2u_3^2(\gamma_2-\gamma_3)^2$$

is a sum of two K-rational squares and hence a norm from $K(\sqrt{-1})$. This again implies that $((u_2^2\gamma_2^2+u_3^2\gamma_3^2)(u_2^2+u_3^2), -1) = 1$, so that $E_{C/K} = 1$. □

10.1 | Special families $\mathcal{F}$, $\mathcal{F}_{C2D4}$

It will be convenient to have a family of curves defined over $\mathbb{Q}_2$ with good ordinary reduction and all roots defined over $\mathbb{Q}_2$. Theorem 10.3 excludes these.

Notation 10.4. For a finite extension $K/\mathbb{Q}_2$, we write $\mathcal{F}$ for the family of genus 2 curves $C : y^2 = cf(x)$ with $c \equiv -1 \bmod 2^3$ and for which $f(x)$ factors as $\prod(x-\alpha_i)(x-\beta_i)$ with

$$\alpha_1 \equiv -5, \quad \beta_1 \equiv 5, \quad \alpha_2 \equiv -4, \quad \beta_2 \equiv -12, \quad \alpha_3 \equiv 2, \quad \beta_3 \equiv -6,$$

the congruences taken modulo 2^8.

We write $\mathcal{F}_{C2D4}$ for the family of C2D4 curves that satisfy these congruences with respect to their given C2D4 structure. (In other words, C satisfies the above congruences 'with its given ordering of roots'.)

Theorem 10.5. *Let $K/\mathbb{Q}_2$ be a finite extension and $C \in \mathcal{F}_{C2D4}$ a C2D4 curve. Then*

(1) *C/K has good ordinary reduction,*
(2) *the Richelot dual curve $\widehat{C}$ has good reduction,*
(3) *the kernel of the Richelot isogeny is contained in the kernel of reduction on* Jac $C(\bar{K})$,
(4) $E_{C/K} = 1$,
(5) *Conjecture 1.14 holds for C/K.*

Proof.

(1) The transformation $x_2 = \frac{x}{2}, y_2 = \frac{y}{8} + \frac{x^2}{8} + \frac{x}{4}$ gives a model C' whose reduction is $y_2^2 + x_2^2 y_2 + x_2 y_2 = x_2^6 + x_2^4 + 1$. Over $\mathbb{F}_2$, this curve is smooth with local polynomial $1 - T^2 + 4T^4$, and is therefore good ordinary over every extension of $\mathbb{F}_2$.
(2) Computing the model for $\widehat{C}$ as in Definition 2.1 and applying the substitutions $x_2 = \frac{x}{2}$ and $y_2 = \frac{y}{16} + \frac{x^2}{8} + \frac{x}{4}$ gives a model that reduces to $y_2^2 + x_2^2 y_2 + y_2 x_2 = x_2^5 + x_2^3 + x_2^2 + x_2$.
(3) Using the change of variables in the proof of (1), one checks that the 2-torsion points on Jac C given by $[(\alpha_i, 0), (\beta_i, 0)]$ map to points on Jac C' that reduce to 0.
(4) Direct computation shows that, up to multiplying by elements that are 1 mod 8, C has $\Delta = 84$, $\ell_1 = -12$, $\ell_2 = -4$, $\ell_3 = -16$, $\delta_1 = 25$, $\delta_2 = 64$, $\delta_3 = 64$, $\hat{\delta}_1 = -\frac{1}{7}$, $\hat{\delta}_2 = -924$, $\hat{\delta}_3 = -4284$, $\eta_1 = 8$, $\eta_2 = 110$, $\eta_3 = -10$, $\xi = 10\,196$, $\delta_2 + \delta_3 = 128$, $\delta_2\eta_2 + \delta_3\eta_3 = 6400$, $\hat{\delta}_2\eta_3 + \hat{\delta}_3\eta_2 = -419\,160$. As elements that are 1 mod 8 are squares, this gives $E_{C/K} = 1$.
(5) C and C' are not deficient by (1, 2), so by Theorem A.1, $\lambda_{C/K} = 1$. By (1) $w_{C/K} = 1$, and by (4) $E_{C/K} = 1$, which proves the result. □

11 | DEFORMING C2D4 CURVES

As explained in §1.4, we will not attempt to prove other cases of Conjecture 1.14 by direct computation, as there are several hundred possible cluster pictures corresponding to semistable C2D4 curves. Instead, we will exploit the fact that we already have a good supply of C2D4 curves over number fields for which we have proved the 2-parity conjecture (through Conjecture 1.14 and Theorem 1.15) and use Lemma 1.19. For this, we will need to be able to approximate C2D4 curves over local fields by curves over number fields, which are well behaved at all other places. In this section, we prove two results that will let us do this (see Theorems 11.15 and 11.16). Roughly speaking, they say that:

- a C2D4 curve C/K_v can be approximated by a curve C'/K such that Conjecture 1.14 holds for C/K_v if and only if it holds for C'/K_v, and moreover, holds for C'/K_w for all $v \neq w$;
- a curve with two C2D4 structures C/K_v can be similarly approximated by C/K admitting two C2D4 structures.

In §12, this will let us show that Conjecture 1.14 is independent of the choice of C2D4 model for a curve C, and moreover, it holds with respect to one C2D4 structure if and only if it holds with respect to another (Theorems 12.1 and 12.3). These, in turn, will let us complete our proof of Theorem 1.16 on Conjecture 1.14 and deduce our main results on the 2-parity and parity conjectures in §13.

11.1 | Continuity of local invariants

Definition 11.1. Let C, C' be two C2D4 curves over a local field of characteristic 0. We will say that C and C' are *ϵ-close* if the leading coefficients and roots of their defining polynomials satisfy $|\alpha_i - \alpha_i'|, |\beta_i - \beta_i'|, |c - c'| < \epsilon$ for $i = 1, 2, 3$.

For curves with $\mathcal{P}, \Delta, \eta_1, \mathcal{P}', \Delta', \eta_1' \neq 0$, we will say that they are *arithmetically* close if

$$w_{C/K} = w_{C'/K}, \quad \lambda_{C/K} = \lambda_{C'/K}$$

and

$$\frac{\delta_1}{\delta_1'} \equiv \frac{\delta_2\delta_3}{\delta_2'\delta_3'} \equiv \frac{\delta_2+\delta_3}{\delta_2'+\delta_3'} \equiv \frac{\eta_2\eta_3}{\eta_2'\eta_3'} \equiv \frac{\hat\delta_2\hat\delta_3}{\hat\delta_2'\hat\delta_3'} \equiv \frac{\eta_1}{\eta_1'} \equiv \frac{\xi}{\xi'} \equiv \frac{\ell_1^2}{\ell_1'^2} \equiv \frac{\ell_1/\Delta}{\ell_1'/\Delta'} \equiv$$
$$\equiv \frac{c}{c'} \equiv \frac{\delta_2\eta_2+\delta_3\eta_3}{\delta_2'\eta_2'+\delta_3'\eta_3'} \equiv \frac{\hat\delta_2\eta_3+\hat\delta_3\eta_2}{\hat\delta_2'\eta_3'+\hat\delta_3'\eta_2'} \equiv 1 \bmod \pi_K$$

for $K/\mathbb{Q}_p$ finite with p odd; the congruence taken mod $4\pi_K$ instead for $p=2$; for $K \cong \mathbb{R}$, we require that all these ratios are positive, and have no requirement for $K \cong \mathbb{C}$.

Lemma 11.2. *For C2D4 curves C over a local field K of characteristic 0, the invariants δ_1, δ_2, δ_3, η_1, η_2, η_3, $\hat\delta_2$, $\hat\delta_3$, ξ, ℓ_1^2, Δ and $w_{C/K}$ are continuous in the roots $\alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3, \beta_3$, and the leading coefficient c. If $\Delta \neq 0$, so are $\frac{\ell_1}{\Delta}$ and $\lambda_{C/K}$.*

Proof. This is clear for all the invariants except possibly w and λ, as they are rational functions in the roots and the leading coefficient c. For archimedean K, $w=1$, while λ is a locally constant function in the roots and c by Lemmata 3.4 and 3.5 and the first paragraph of the proof of Theorem 5.2. For K non-archimedean, the special fibre of the minimal regular model of C/K^{nr} (with Frobenius action) is locally constant, and hence, so is the deficiency term $\mu_{C/K}$ (cf. [15, Lemma 12.3]) and the local Tamagawa number $c_{\mathrm{Jac}\, C/K}$ (cf. [5, Thm. 2.3]); the coefficients of the equation of the dual curve $\widehat{C}$ are continuous in the roots and in c, so λ is also locally constant. The Galois representation $T_\ell(\mathrm{Jac}\, C) \cong H^1_{et}(C/K, \mathbb{Z}_\ell)(1)$ is also locally constant ([21, p.569]), and hence so is the root number $w_{C/K}$. □

Lemma 11.3. *Let C be a C2D4 curve over a local field of characteristic 0 with $\mathcal{P}, \Delta, \eta_1 \neq 0$. Then there exists $\epsilon > 0$ such that every C2D4 curve that is ϵ-close to C is arithmetically close to C.*

Proof. Clear from Lemma 11.2. □

Lemma 11.4. *Let C, C' be arithmetically close C2D4 curves over a local field of characteristic 0 with $\mathcal{P}$, Δ, η_1, $\mathcal{P}'$, Δ', $\eta_1' \neq 0$. Then Conjecture 1.14 holds for C if and only if it holds for C'.*

Proof. Clear as λ and w are the same, and the terms in the Hilbert symbols in $E_{C/K}$ change by squares. □

Remark 11.5. If t is sufficiently close to 0, then C_t is ϵ-close to C. More generally, if the coefficients of $m(z) = \frac{\mathbf{a}z+\mathbf{b}}{\mathbf{c}z+\mathbf{d}}$ are sufficiently close to $\mathbf{a}=\mathbf{d}=1, \mathbf{b}=\mathbf{c}=0$, then C_m is ϵ-close to C (see Definitions 6.1 and 6.3).

11.2 | D4 quartics

To approximate C2D4 curves over p-adic fields by curves over number fields $y^2 = cf(x)$, we must ensure that the Galois group of $f(x)$ does not become too large. We will also want to ensure that the new curve is well behaved at all other primes.

Lemma 11.6. *A separable monic quartic polynomial $q(x)$ over a field K has* $\mathrm{Gal}(q(x)) \subseteq D_4$ *if and only if its roots are of the form*

$$r_1 = z_1 + z_2\sqrt{a} + z_3\sqrt{b+d\sqrt{a}} + z_4\sqrt{a}\sqrt{b+d\sqrt{a}},$$

$$r_2 = z_1 + z_2\sqrt{a} - z_3\sqrt{b+d\sqrt{a}} - z_4\sqrt{a}\sqrt{b+d\sqrt{a}},$$

$$r_3 = z_1 - z_2\sqrt{a} - z_3\sqrt{b-d\sqrt{a}} + z_4\sqrt{a}\sqrt{b-d\sqrt{a}},$$

$$r_4 = z_1 - z_2\sqrt{a} + z_3\sqrt{b-d\sqrt{a}} - z_4\sqrt{a}\sqrt{b-d\sqrt{a}},$$

for some $a \in K^\times$ and $b, d, z_1, z_2, z_3, z_4 \in K$.

Proof. Clearly, a quartic with such roots has Galois group $\subseteq D_4$. For the converse, if the Galois group contains a 4-cycle, the result is clear. If it is contained in the Klein group V_4, the result follows from Lemma 11.10 below by taking $d = 0$. If it is either trivial or C_2 acting by a transposition, the result follows by taking $a = 1$ and $d = b - 1$. □

Lemma 11.7. *Let K be a local field of odd residue characteristic and $q(x)$ as in Lemma 11.6. If $a, b, d, z_1, z_2, z_3, z_4 \in \mathcal{O}_K$ and either $16(b^2 - ad^2)(z_3^2 - az_4^2)^2$ or $2az_2^2 - bz_3^2 - 2adz_3z_4 - abz_4^2$ is a unit, then $\bar{q}(x)$ does not have roots of multiplicity $\geqslant 3$.*

Proof. One checks that $(r_1 - r_2)^2(r_3 - r_4)^2 = 16(b^2 - ad^2)(z_3^2 - az_4^2)^2$ and

$$\frac{1}{4}(r_1 - r_2)^2(r_3 - r_4)^2 + (r_1 - r_3)(r_1 - r_4)(r_2 - r_3)(r_2 - r_4) = 4(2az_2^2 - bz_3^2 - 2adz_3z_4 - abz_4^2)^2.$$

□

Remark 11.8. $(r_1 - r_3)(r_2 - r_4) + (r_2 - r_3)(r_1 - r_4) = 4(2az_2^2 - bz_3^2 - 2adz_3z_4 - abz_4^2)$.

Lemma 11.9. *Let K be a number field and S a finite set of places of K including all primes above 2, but excluding at least one infinite place. For each $v \in S$, let $q_v(x) \in \mathcal{O}_{K_v}[x]$ (or $\in K_v[x]$ for $v|\infty$) be*

a monic quartic with $\mathrm{Gal}(q_v(x)) \subseteq D_4$. *There exists a monic quartic* $q(x) \in \mathcal{O}_K[x]$ *with* $\mathrm{Gal}(q(x)) \subseteq D_4$ *such that*

(i) *for each* $v \in S$, *the roots of* $q(x)$ *are arbitrarily close to those of* $q_v(x)$ *(with respect to an ordering that respects the* D_4*-action),*
(ii) *for all* $v \notin S$, $q(x) \bmod v$ *has no roots of multiplicity* $\geqslant 3$.

Proof. For each $v \in S$, write the roots of q_v as in Lemma 11.6 with parameters $a_v, b_v, d_v, z_{1,v}, z_{2,v}, z_{3,v}, z_{4,v} \in K_v$. Note that any monic polynomial $q(x) \in K[x]$ in the form of Lemma 11.6 whose parameters are v-adically close to those of $q_v(x)$ satisfies (i).

Use strong approximation (and the infinite place outside S) to choose $a, b, d, z_1, z_2, z_3, z_4 \in K$ that lie in $\mathcal{O}_{K_v}$ for primes $v \notin S$ as follows. First choose any b, d, z_1, z_3, z_4 that are v-adically close to $b_v, d_v, z_{1,v}, z_{3,v}, z_{4,v}$ for $v \in S$. Now choose a that is v-adically close to a_v for $v \in S$ with $\gcd(a, bz_3)$ supported on S; this ensures that if a prime $w \notin S$ divides $(b^2 - ad^2)(z_3^2 - az_4^2)$ then $w \nmid a$. Finally, choose z_2 that is v-adically close to $z_{2,v}$ for $v \in S$ such that for primes $w \notin S$ that divide $(b^2 - ad^2)(z_3^2 - az_4^2)$, the expression $2az_2^2 - bz_3^2 - 2az_3z_4 - abz_4^2$ is a w-adic unit. By Lemma 11.7, $q(x)$ now satisfies (ii).

Finally, note that as $q(X)$ lies in $\mathcal{O}_{K_v}[x]$ both for $v \in S$ (by (i)) and $v \notin S$ (by construction), it lies in $\mathcal{O}_K[x]$. □

11.3 | V4 quartics

We will need a similar result for quartics with Galois group V_4. Recall that for us V_4 consists of double transpositions.

Lemma 11.10. *A separable monic quartic polynomial* $q(x)$ *over a field* K *has* $\mathrm{Gal}(q(x)) \subseteq V_4$ *if and only if its roots are of the form*

$$r_1 = z_1 + z_2\sqrt{a} + z_3\sqrt{b} + z_4\sqrt{ab}, \qquad r_2 = z_1 - z_2\sqrt{a} + z_3\sqrt{b} - z_4\sqrt{ab},$$

$$r_3 = z_1 + z_2\sqrt{a} - z_3\sqrt{b} - z_4\sqrt{ab}, \qquad r_4 = z_1 - z_2\sqrt{a} - z_3\sqrt{b} + z_4\sqrt{ab},$$

for some $a, b \in K^\times$ *and* $z_1, z_2, z_3, z_4 \in K$.

Proof. Clearly, a quartic with such roots has Galois group $\subseteq V_4$. Conversely, the splitting field of a quartic with $\mathrm{Gal}\, q(x) \subseteq V_4$ is of the form $K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K^\times$; the z_i are then found by solving the given linear system of equations for the r_i. □

Lemma 11.11. *Let* K *be a local field of odd residue characteristic and* $q(x)$ *as in Lemma 11.10. If* $a, b, z_1, z_2, z_3, z_4 \in \mathcal{O}_K$ *and either* $a(z_2^2 - bz_4^2)$ *or* $b(z_3^2 - bz_4^2)$ *is a unit, then* $\bar{q}(x)$ *does not have roots of multiplicity* $\geqslant 3$.

Proof. One checks that $(r_1 - r_2)(r_3 - r_4) = 4a(z_2^2 - bz_4^2)$ and $(r_1 - r_3)(r_2 - r_4) = 4b(z_3^2 - az_4^2)$. □

Lemma 11.12. *Let* K *be a number field and* S *a finite set of places of* K *including all primes above 2, but excluding at least one infinite place. For each* $v \in S$, *let* $q_v(x) \in \mathcal{O}_{K_v}[x]$ *(or* $\in K_v[x]$ *for* $v|\infty$*)*

be a monic quartic with $\mathrm{Gal}(q_v(x)) \subseteq V_4$. *There exists a monic quartic* $q(x) \in \mathcal{O}_K[x]$ *with* $\mathrm{Gal}(q(x)) \subseteq V_4$ *such that*

(i) *for each* $v \in S$, *the roots of* $q(x)$ *are arbitrarily close to those of* $q_v(x)$,
(ii) *for all* $v \notin S$, $q(x) \bmod v$ *has no roots of multiplicity* $\geqslant 3$.

Proof. The proof is the same as for Lemma 11.9, except that the parameters $a, b, z_1, z_2, z_3, z_4 \in K$ (lying in $\mathcal{O}_{K_v}$ for $v \notin S$) are chosen as follows. First choose z_1 and a to be v-adically close to $z_{1,v}$ and a_v for $v \in S$. Choose z_3 and b to be v-adically close to $z_{3,v}$ and b_v for $v \in S$ such that $\gcd(a, bz_3)$ is supported on S — this ensures that for primes $v \notin S$ that divide a, $b(z_3^2 - az_4^2)$ is a unit. Choose z_2 to be v-adically close to $z_{2,v}$ for $v \in S$ such that $\gcd(b, z_2)$ is supported on S and $az_2^2 \neq bz_3^2$ — in particular, this ensures that for primes $v \notin S$ that divide b, $a(z_2^2 - bz_4^2)$ is a unit. Finally, choose z_4 to be v-adically close to $z_{4,v}$ for $v \in S$ such that $\gcd(az_2^2 - bz_3^2, z_4)$ is supported on S — this ensures that for primes $v \notin S$ that do not divide ab either $(z_2^2 - bz_4^2)$ or $(z_3^2 - az_4^2)$ is a unit. By Lemma 11.11, $q(x)$ now satisfies (ii). □

11.4 | Glueing a quadratic to a polynomial

Lemma 11.13. *Let* K *be a number field and* $q(x) \in \mathcal{O}_K[x]$ *be a separable monic polynomial. Let* S *be a finite set of places of* K *including all primes above 2 and all primes with residue field of size less than* $\deg q(x) + 2$, *but excluding at least one infinite place. For each* $v \in S$, *let* $h_v(x) \in \mathcal{O}_{K_v}[x]$ *(or* $\in K_v[x]$ *for* $v|\infty$*) be a monic quadratic. There exists a monic quadratic* $h(x) \in \mathcal{O}_K[x]$ *such that*

(1) *for each* $v \in S$, *the coefficients of* $h(x)$ *are arbitrarily close to those of* $h_v(x)$, *and*
(2) *for each prime* $v \notin S$, $h(x)q(x) \bmod v$ *has either (a) no repeated roots or exactly one double root in the residue field* $\overline{\mathbb{F}}_v$, *or (b) all its repeated roots coming from those of* $q(x) \bmod v$.

Proof. Write $h_v(x) = x^2 + a_v x + b_v$. Using strong approximation (and the infinite place outside of S), pick $a \in \mathcal{O}_K$ that is v-adically close to the a_v for all $v \in S$ and such that $P = \prod(a + r + r') \neq 0$, the product taken over all pairs of roots of $q(x)$ (including repeats).

Let T be the set of primes outside S that divide $P \cdot \mathrm{Disc}(q(x))$.

Using strong approximation now pick $b \in \mathcal{O}_K$ so that

(i) b is v-adically close to b_v for all $v \in S$, and
(ii) $x^2 + ax + b \bmod v$ is separable and coprime to $q(x) \bmod v$ for all $v \in T$.

The fact that the residue field at $v \notin S$ has size at least $\deg q(x) + 2$ ensures that for each $a \bmod v$, there is always a polynomial over $\mathbb{F}_v$ that satisfies (ii).

We can now take $t(x) = x^2 + ax + b$. Indeed, condition (ii) ensures that

- if $q(x) \bmod v$ has a double root, then the roots of $h(x) \bmod v$ are distinct from each other and from the roots of $q(x) \bmod v$;
- the roots of $h(x) \bmod v$ cannot both coincide with roots of $q(x) \bmod v$ for any $v \notin S$: otherwise, we would have $P \equiv 0 \bmod v$, so that $v \in T$, which contradicts (ii);
- if $h(x) \bmod v$ has a double root (this would then be $\equiv -a/2 \bmod v$) for $v \notin S$, then it does not coincide with a root of $q(x) \bmod v$. □

11.5 | Approximating a curve

Lemma 11.14. *Let K be a finite extension of $\mathbb{Q}_p$ for an odd prime p. There are polynomials $f_1(x)$ and $f_2(x)$ of the form $f(x) = r(x)s(x)t(x)$ with $r(x), s(x), t(x) \in \mathcal{O}_K[x]$ monic quadratic and $\mathrm{Gal}(\bar{K}/K)$ acting on the roots of $s(x)t(x)$ as a subgroup of V_4, such that*

(1) *$f_1(x)$ has cluster picture*  , *and*
(2) *$f_2(x)$ has cluster picture*  *and $v(\alpha_2+\beta_2-\alpha_3-\beta_3) = 1$,*

where , *(α_2, β_2) and* *(α_3, β_3) denote the roots of r, s and t, respectively.*

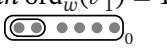
Proof. Since $s(x), t(x) \in K[x]$, the constraint on $\mathrm{Gal}(\bar{K}/K)$ means that its elements will either act trivially on the roots of $s(x)t(x)$ or simultaneously swap the roots of $s(x)$ and of $t(x)$.

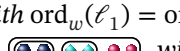
(1) Take $r(x) = x(x-1)$ and $s(x)$, $t(x)$ quadratics whose images over the residue field $k(x)$ are distinct and irreducible (these exist even when $k = \mathbb{F}_3$).
(2) Take $r(x) = x(x-1)$, $s(x) = (x-\pi)(x-\pi-1)$, $t(x) = (x+\pi)(x+\pi-1)$, where $\pi = \pi_K$ is a uniformiser. □

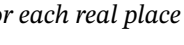
Theorem 11.15. *Let K be a number field. Let v be a place of K and C_v/K_v be a C2D4 curve with $\mathcal{P}, \Delta, \eta_1 \neq 0$. Let $v' \neq v$ be an archimedean place of K.*

For every $\epsilon > 0$, there is a C2D4 curve C/K with $\mathcal{P}, \Delta, \eta_1 \neq 0$ such that

(i) *C/K_v and C_v/K_v are ϵ-close,*
(ii) *for each prime $w \neq v$ with $w|2$, the C2D4 curve C/K_w lies in $\mathcal{F}_{C2D4}$;*
(iii) *for each prime $w \neq v$ with $w \nmid 2$, the curve C/K_w is semistable with cluster picture*
-  *or* , *or*
- 

with $\mathrm{ord}_w(\ell_1) = 1$, *or*
- 

with $\mathrm{ord}_w(\ell_1) = \mathrm{ord}_w(\ell_2) = \mathrm{ord}_w(\ell_3) = \mathrm{ord}_w(\eta_2) = \mathrm{ord}_w(\eta_3) = 0$, *or*
-  *with* $\mathrm{ord}_w(\ell_1) = \mathrm{ord}_w(\ell_2) = \mathrm{ord}_w(\ell_3) = 0$, *or*
- 

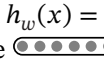
with $\mathrm{ord}_w(\ell_1) = \min(n, m)$, $\mathrm{ord}_w(\ell_2) = \mathrm{ord}_w(\ell_3) = \mathrm{ord}_w(\eta_2) = \mathrm{ord}_w(\eta_3) = 0$;
(iv) *for each real place $w \neq v, v'$, the curve C/K_w has picture*  .

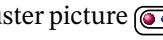
Proof. Note that being ϵ-close to C_v/K_v for sufficiently small ϵ guarantees that $\mathcal{P}, \Delta, \eta_1 \neq 0$ (Lemma 11.2), so this condition will be automatic.

Write C_v/K_v as $y^2 = c_v \cdot h_v(x)q_v(x)$ with $h_v(x)$ a monic quadratic and $q_v(x)$ a monic quartic with $\mathrm{Gal}(q_v(x)) \leqslant D_4$ given by the C2D4 structure. In the case that v is non-archimedean, we may assume that $h_v(x), q_v(x) \in \mathcal{O}_{K_v}[x]$: otherwise scale x by a suitable totally positive element of K whose only prime factor is v (this exists as v has finite order in the class group).

Let S be the set consisting of v, all real places other than v', primes above 2 and all primes with residue field of size < 23. For $w \in S \setminus \{v\}$, define C2D4 curves $C_w^{spc} : y^2 = c_w h_w(x) q_w(x)$ over K_w for quadratic $h_w(x)$ and quartic $q_w(x)$ as follows:

- For $w|\infty$, let $c_w = -1$ and $h_w(x) = x(x-1)$, $q_w(x) = \prod_{i=2}^{5}(x-i)$, so C_w^{spc} has picture  .

- For $w|2$, let $c_w = 1$ and $h_w(x) = r(x)$, $q_w(x) = s(x)t(x)$ for r, s, t given by the roots in Definition 10.4, so $C_w^{spc} \in \mathcal{F}_{C2D4}$.
- For $w \nmid 2\infty$, let $c_w = 1$ and $h_w(x) = r(x), q_w(x) = s(x)t(x)$ for r, s, t given by Lemma 11.14(i); in particular, C_w^{spc} has picture  .

Pick $c \in K$ such that $c = c_w \cdot \square \in K_w^\times$ for all $w \in S$. Let S' be the set of primes $w \notin S$ such that $\mathrm{ord}_w(c)$ is odd. For these primes, define $C_w^{spc} : y^2 = ch_w(x)q_w(x)$ by setting $h_w(x) = r(x)$ and $q_w(x) = s(x)t(x)$ for r, s, t given in Lemma 11.14(ii); these curves have cluster picture  with $\mathrm{ord}_w(\ell_1) = 1$.

Using Lemmata 11.9 and 11.13, construct a monic D_4 quartic $q(x) \in \mathcal{O}_K[x]$ and monic C_2 quadratic $h(x) \in \mathcal{O}_K[x]$ such that the C2D4 curve $C : y^2 = ch(x)q(x)$

(1) is $\frac{\epsilon}{2}$-close to C_v/K_v,
(2) is close to C_w^{spc}/K_w for $w \in S \cup S' \setminus \{v\}$,
(3) has picture  ,  ,  or  for $w \notin S \cup S'$.

By the semistability criterion (Theorem 2.12), C/K_w is semistable at all $w \neq v$ with $w \nmid 2$.

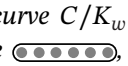
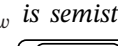
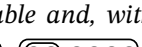
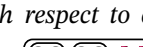
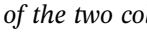
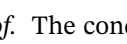
It remains to ensure that the invariants listed under (iii) are units. Centre the curve C by a substitution $x \mapsto x + \lambda$ to give a curve C'. Using strong approximation and Theorem 6.6, pick $t \in K$ such that (a) for $w \in S$, t is w-adically close to 0, and (b) for finite $w \notin S$ where C has cluster picture  or  or  or  , C_t has the same cluster picture and the invariants of C_t specified in (iii) are units. Note that at all other places C_t will have cluster picture  or  by Theorem 2.17. Finally, shifting C_t back by $x \mapsto x - \lambda$ gives the required curve C''. □

11.6 | Approximating a curve with two isogenies

Theorem 11.16. *Let K be a number field and v a place of K. Let $C_v : y^2 = c_v f_v(x)$ be a curve over K_v that admits two C2D4 structures, $C_v^{(1)}$ and $C_v^{(2)}$, each of which has $\mathcal{P}, \Delta, \eta_1 \neq 0$. Let $v' \neq v$ be an archimedean place of K. Suppose that one of the following two conditions holds:*

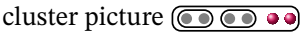
(1) • *the second colouring is obtained from the first by relabelling colours, and*
  • $\mathrm{Gal}(f_v)$ *preserves colours; or*
(2) • *both colourings have the same ruby roots, and*
  • $\mathrm{Gal}(f_v)$ *acts on the sapphire and turquoise roots as a subgroup of V_4.*

Then for every $\epsilon > 0$, there is a curve $C : y^2 = cf(x)$ over K that admits two C2D4 structures, $C^{(1)}$ and $C^{(2)}$, such that

(i) *$C^{(1)}/K_v$ and $C_v^{(1)}/K_v$ are ϵ-close, and $C^{(2)}/K_v$ and $C_v^{(2)}/K_v$ are ϵ-close,*
(ii) *for each prime $w \neq v$ with $w|2$, the curve C/K_w lies in $\mathcal{F}$,*
(iii) *for each prime $w \neq v$ with $w \nmid 2$, the curve C/K_w is semistable and, with respect to each of the two colourings, has cluster picture*  ,  ,  ,  *or*  .
(iv) *for each real place $w \neq v, v'$, the curve C/K_w has picture*  , , , *or*  , *with respect to both colourings.*

Proof. The condition on the colourings and the Galois action in (1) is equivalent to saying that $f_v(x)$ factorises into three quadratics $a_v(x)b_v(x)d_v(x)$ over K_v and that (for both C2D4 structures)

the roots of each quadratic are monochromatic. The condition in (2) is equivalent to a factorisation into a quadratic $r_\upsilon(x)$ with the ruby roots and a quartic $q_\upsilon(x)$ whose Galois group is contained in V_4. Thus, to prove the theorem, it will suffice to construct C/K so that

- it satisfies (ii), (iv) and (iii), avoiding the cluster picture  in case (1), and
- in case (1), $f(x)$ admits a factorisation into three quadratics $a(x)b(x)d(x)$ over K and $c, a(x), b(x), d(x)$ are υ-adically close to $c_\upsilon, a_\upsilon(x), b_\upsilon(x), d_\upsilon(x)$,
- in case (2), $f(x)$ admits a factorisation over K into a quadratic $r(x)$ and a quartic $q(x)$ with Galois group inside V_4, and $c, r(x), q(x)$ are υ-adically close to $c_\upsilon, r_\upsilon(x), q_\upsilon(x)$.

Indeed, such a curve will automatically admit two C2D4 structures that satisfy (i).

The construction of C/K follows exactly as in the proof of Theorem 11.15, except that the use of Lemmata 11.9 and 11.13 in the penultimate paragraph is replaced by two applications of Lemma 11.13 in case (1) and by Lemmata 11.12 and 11.13 in case (2), and that the step in the final paragraph is not relevant here. □

11.7 | Making the terms $\mathcal{P}, \eta_1, \Delta \neq 0$

Recall that we will eventually need to address the special cases when $\mathcal{P}, \eta_1$, or Δ is 0. Here we record the methods to make small perturbations to the given C2D4 model to make these invariants non-zero.

Lemma 11.17. *Let K be a local field of characteristic 0 and C/K a centred C2D4 curve. Then there is a $t_0 \in K$ arbitrarily close to 0 such that for all $t \in K$ sufficiently close to t_0 the model C_t has $\mathcal{P} \neq 0$.*

Proof. It suffices to find one value of t_0 close to 0 such that C_{t_0} has $\mathcal{P} \neq 0$, since $\mathcal{P}(C_t)$ is continuous as a function of t. By definition $\mathcal{P} = \ell_1\ell_2\ell_3\eta_2\eta_3\xi(\delta_2+\delta_3)(\delta_2\eta_2+\delta_3\eta_3)(\hat\delta_2\eta_3+\hat\delta_3\eta_2)$. As the individual factors are rational functions in t, it suffices to prove that none of them are identically zero for $t \in \bar K$.

Consider a Möbius transformation of the form $m : z \mapsto \mathbf{c}(\frac{1}{z-\mathbf{a}} - \mathbf{b})$, where $\mathbf{b}$ and $\mathbf{c}$ are chosen so that $m(\alpha_1) = \alpha_1$ and $m(-\alpha_1) = -\alpha_1$. By Lemma 6.4, $m = M_t$ for some $t \in \bar K$. If $\mathbf{a}$ is chosen to be sufficiently close but not equal to α_2, then $|M_t(\alpha_2)| \gg |M_t(\pm\alpha_1)|, |M_t(\alpha_3)|, |M_t(\beta_2)|, |M_t(\beta_3)|$. This guarantees that $\ell_1, \ell_3, \eta_2, \delta_2+\delta_3, \delta_2\eta_2+\delta_3\eta_3 \neq 0$ for C_t. Note also that taking $\mathbf{a}$ close to α_2 keeps $\frac{1}{\mathbf{c}}(M_t(\beta_2) \pm M_t(\alpha_1)) = \frac{\pm\alpha_1-\beta_2}{(\pm\alpha_1-\mathbf{a})(\beta_2-\mathbf{a})}$ away from 0, which ensures that $\hat\delta_2\eta_3+\hat\delta_3\eta_2 = \alpha_2^4(\beta_2-\alpha_1)(\beta_2+\alpha_1)+\mathcal{O}(\alpha_2^3)$ also becomes non-zero for C_t.

Similarly, picking $\mathbf{a}$ close to α_3 shows that one can make $\ell_2, \eta_3 \neq 0$.

Finally, for ξ embed $K \subset \mathbb{C}$ and take $\mathbf{a} \approx \alpha_1$: this makes $\xi(C_t)$ arbitrarily close to $-32\alpha_1^4$ in $\mathbb{C}$, and hence non-zero. □

Remark 11.18. One cannot similarly change the model to make either η_1 or Δ non-zero. A computation shows that if $\eta_1(C) = 0$, then $\eta_1(C_t) = 0$ for all t. Moreover, $\Delta(C) = 0$ if and only if $\Delta(C_m) = 0$ for every $m \in \mathrm{GL}_2(K)$, so, by Remark 6.2, the condition '$\Delta = 0$' is independent of the choice of model.

Lemma 11.19. *Let K be a local field of characteristic 0, and $C : y^2 = cf(x)$ a C2D4 curve over K with $\mathcal{P}, \Delta \neq 0$.*

(i) *For every $\epsilon > 0$, there exists another C2D4 curve $C' : y^2 = cg(x)$ over K whose roots satisfy $|\alpha_i - \alpha_i'|, |\beta_i - \beta_i'| < \epsilon$ and which has $\eta_1(C') \neq 0$.*
(ii) *There is a $\delta > 0$ such that for every C2D4 curve $C' : y^2 = c'g(x)$ over K with $|c - c'|$, $|\alpha_i - \alpha_i'|$, $|\beta_i - \beta_i'| < \delta$, Conjecture 1.14 holds for C/K if and only if it holds for C'/K.*

Proof.

(i) The definition of η_1 only depends on the roots of the quartic in $f(x)$. Write these as in Lemma 11.6 (with $\alpha_2 = r_1$, $\beta_2 = r_3$, $\alpha_3 = r_2$, $\beta_3 = r_4$ to get the Galois action right). By Remark 11.8, $\eta_1 = 4(2az_2^2 - bz_3^2 - 2adz_3z_4 - abz_4^2)$. One checks that since $a \neq 0$ and at least one of z_2, z_3, z_4 is not 0, not all partial derivatives with respect to the parameters are simultaneously 0. Changing the corresponding parameter by a sufficiently small amount gives the required $g(x)$.
(ii) If δ is sufficiently small, then the two curves have the same invariants up to squares (other than η_1), the same local root number and $\lambda_{C/K} = \lambda_{C'/K}$ (Lemma 11.2), and $\eta_1(C')$ is arbitrarily close to $\eta_1(C)$. If either $\eta_1(C) \neq 0$ or $\eta_1(C) = \eta_1(C') = 0$, then the result follows directly, as each Hilbert symbol in Conjecture 1.14 is the same for C and C'.

Suppose $\eta_1(C) = 0$ and $\eta_1(C') \neq 0$. By Lemma 9.9(2), the invariants of C' satisfy $\delta_2\delta_3 = -4\Delta^2\hat{\delta}_1 + \eta_1^2$. If δ is sufficiently small, then η_1 will be close to 0, so that $-\delta_2\delta_3\Delta^2\hat{\delta}_1$ is a perfect square in K. Hence $(\eta_1, -\delta_2\delta_3\Delta^2\hat{\delta}_1) = 1$ for C'/K, which proves that all the Hilbert symbols for C and C' agree in this case too. □

Lemma 11.20. *Let K be a local field of characteristic 0, and $C : y^2 = cf(x)$ a C2D4 curve over K. For every $\epsilon > 0$, there exists another C2D4 curve $C' : y^2 = cg(x)$ over K whose roots satisfy $|\alpha_i - \alpha_i'|, |\beta_i - \beta_i'| < \epsilon$ and which has $\Delta(C') \neq 0$.*

Proof. We may assume that the curve is centred. If $\Delta(C) \neq 0$, the result is clear, so suppose

$$\Delta(C) = -c(\alpha_1^2\ell_1 - \alpha_2\beta_2(\alpha_3 + \beta_3) + \alpha_3\beta_3(\alpha_2 + \beta_2)) = 0.$$

If $\ell_1 \neq 0$, we can obtain a suitable C' by a small perturbation to α_1^2, so suppose $\ell_1 = 0$, that is, $\alpha_2 + \beta_2 = \alpha_3 + \beta_3$. We cannot moreover have $\alpha_2\beta_2 = \alpha_3\beta_3$ as then α_2, β_2 would be the roots of the same quadratic as α_3, β_3 and C would be singular. Thus, the above equation for Δ forces $\alpha_2 = -\beta_2$ and $\alpha_3 = -\beta_3$.

To obtain a suitable C', take $\alpha_1' = \alpha_1$ and shift the other roots by a small $t \in K$, that is, take $\alpha_i' = \alpha_i + t, \beta_i' = \beta_i + t$ for $i = 2, 3$. This preserves the Galois action on roots, so $g(x) \in K[x]$. Moreover, $\ell_1' = \ell_1 = 0$, but now $\alpha_2' + \beta_2' \neq 0$, and so $\Delta(C') \neq 0$, as required. □

Lemma 11.21. *Let K be a local field of characteristic 0 and C/K a curve that admits two C2D4 structures, $C^{(1)}$ and $C^{(2)}$, such that $\mathcal{P}, \Delta \neq 0$ for $C^{(1)}$. Then for every $\epsilon > 0$, there is a C2D4 curve C_2/K that admits two C2D4 structures, $C_2^{(1)}$ and $C_2^{(2)}$, such that $C_2^{(1)}$ is arithmetically and ϵ-close to $C^{(1)}$ and such that $C_2^{(2)}$ has $\mathcal{P}, \Delta \neq 0$.*

Proof. Note that a shift of the x-coordinate $x \mapsto x + \lambda$ does not change $\mathcal{P}$ for either C2D4 structure. Thus, we can take $m = s^{-1} \circ M \circ s$, where s is the shift that centres $C^{(2)}$ and $M \in \mathrm{GL}_2(K)$ close to the identity that then makes $\mathcal{P}(C_{Ms}^{(2)}) \neq 0$ from Lemma 11.17. Now apply Lemma 11.20 to $C_{s^{-1}Ms}$ to obtain C_2. □

12 | MAIN LOCAL THEOREM: GENERAL CASE

We now return to the proof of Conjecture 1.14.

12.1 | Changing the model

Theorem 12.1. *Let K be a local field of characteristic 0. Let C/K be a C2D4 curve with $\mathcal{P}, \Delta \neq 0$. Suppose that C/K admits another C2D4 model C'/K for which Conjecture 1.14 holds. Then Conjecture 1.14 holds for C/K.*

Proof. Write $K = F_v$ as the completion of some number field F at a place v, which also has a complex place $v' \neq v$.

We may change the C2D4 model by scaling the y-coordinate (this changes the leading term c by a square), as this does not affect any of the Hilbert symbols in $E_{C/K}$ and hence the validity of Conjecture 1.14 for C/K. By Remark 6.2, we may therefore assume that the model C' is C_m for some $m \in \mathrm{GL}_2(K)$. Since m and m^{-1} are continuous, by Lemma 11.19, we may moreover assume that $\eta_1 \neq 0$ for both C and C'.

By Theorems 11.15 and 4.1, there is a C2D4 curve $\tilde{C}_m$ defined over F which is arithmetically close to C_m over F_v and for which Conjecture 1.14 holds at all places of F. Moreover, by continuity of m^{-1}, we can pick it to be v-adically sufficiently close to C_m so that $(\tilde{C}_m)_{m^{-1}}$ is arithmetically close to C.

Now use continuity (Lemmata 11.3 and 11.4) and strong approximation to pick $m' \in \mathrm{GL}_2(F)$ such that (i) m' is v-adically close to m^{-1}, so that $\tilde{C} = (\tilde{C}_m)_{m'}$ is arithmetically close to C, and (ii) m' is w-adically close to the identity at all places $w \neq v, v'$ that are either archimedean or where $\tilde{C}_m$ has bad reduction, so that $\tilde{C}$ is arithmetically close to $(\tilde{C}_m)$ at these places.

To summarise, we have now replaced the pair of curves C, C_m defined over K by a pair $\tilde{C}, \tilde{C}_m$ defined over F such that

- C and $\tilde{C}$ are arithmetically close over F_v,
- C_m and $\tilde{C}_m$ are arithmetically close over F_v,
- Conjecture 1.14 holds for $\tilde{C}_m$ at all places of F,
- Conjecture 1.14 holds for $\tilde{C}$ at all places $w \neq v, v'$ of F that are archimedean or where C_m has bad reduction, and hence by Theorem 4.1 at all places $w \neq v$ of F.

By Theorem 1.15, the 2-parity conjecture holds for $\tilde{C}_m/F$. Since $\tilde{C}$ is another model for $\tilde{C}_m$, the 2-parity conjecture also holds for $\tilde{C}/F$. By Lemma 1.19, it follows that Conjecture 1.14 must also hold for $\tilde{C}$ at the remaining place v. Since this curve is arithmetically close to C over $K = F_v$, the conjecture also holds for C/K, as required. □

12.2 | Finite places

Theorem 12.2. *Let K be a finite extension of $\mathbb{Q}_p$ and C/K a C2D4 curve with $\mathcal{P}, \Delta \neq 0$. Then Conjecture 1.14 holds for C/K if either*

(1) *p is odd and C/K is semistable with cluster picture*  ,  ,  ,  ,  ,  ,  *or*  , *or*

(2) *$p = 2$, C/K has good ordinary reduction and the kernel of the associated Richelot isogeny on the Jacobian is precisely the kernel of the reduction map on 2-torsion points.*

Proof. We consider the cases of odd and even residue characteristic independently. By Lemma 11.19, we may assume that $\eta_1 \neq 0$. By Lemma 3.7, we may assume that the residue field of K is sufficiently large. The result now follows from Theorems 4.1, 6.6 and 12.1 for p odd, and from Proposition 10.2 and Theorems 10.3 and 12.1 for $p = 2$. □

12.3 | Changing the isogeny

Theorem 12.3. *Let K be a non-archimedean local field of characteristic 0. Let $C : y^2 = cf(x)$ be a curve over K that admits two C2D4 structures, $C^{(1)}$ and $C^{(2)}$, both of which have $\mathcal{P}, \Delta \neq 0$ and such that Conjecture 1.14 holds for $C^{(1)}$. Suppose that one of the following two conditions holds:*

(1)
- *the second colouring is obtained from the first by relabelling colours, and*
- *$\mathrm{Gal}(f)$ preserves colours; or*

(2)
- *both colouring have the same ruby roots, and*
- *$\mathrm{Gal}(f)$ acts on the sapphire and turquoise roots as a subgroup of V_4.*

Then Conjecture 1.14 holds for $C^{(2)}$.

Proof for K a finite extension of $\mathbb{Q}_2$. Since the validity of Conjecture 1.14 is unchanged by going to an unramified extension of odd degree (Lemma 3.7), we may assume that $[K : \mathbb{Q}_2] > 1$.

Pick a number field F that has a prime υ above 2 with completion $F_\upsilon \simeq K$, and such that F has no other primes above 2 and has a complex place. (To see that such a field exists, pick a primitive generator θ for $K/\mathbb{Q}_2$ and approximate its minimal polynomial by a polynomial $m(x) \in \mathbb{Q}[x]$ that has at least two complex roots; then $F = \mathbb{Q}[x]/m(x)$ has the required property.)

Over local fields, a small perturbation to the coefficients of a separable polynomial does not change its Galois group, so by Lemma 11.19, we may assume that both curves have $\eta_1 \neq 0$. By Theorems 11.16 and 4.1, there is a curve $\tilde{C}/F$ that admits two C2D4 structures $\tilde{C}^{(1)}$ and $\tilde{C}^{(2)}$ such that $\tilde{C}^{(i)}$ is close to $C^{(i)}$ and such that Conjecture 1.14 holds for both $\tilde{C}^{(1)}$ and $\tilde{C}^{(2)}$ at all places $w \neq \upsilon$. In particular, Conjecture 1.14 holds for $\tilde{C}^{(1)}$ at all places of F, and hence, the 2-parity conjecture holds for $\tilde{C}$ (Theorem 1.15). It thus also holds for $\tilde{C}^{(2)}$, and thus, by Lemma 1.19, it follows that Conjecture 1.14 must hold for $\tilde{C}^{(2)}/F_\upsilon$, and hence for $C^{(2)}/K$. □

12.4 | 2-adic places

Theorem 12.4. *Let K be a finite extension of $\mathbb{Q}_2$. Suppose that C/K lies in $\mathcal{F}$. Then Conjecture 1.14 holds for every C2D4 structure on C/K with $\mathcal{P}, \Delta \neq 0$.*

Proof. The curve $C : y^2 = cf(x)$ has all its Weierstrass points defined over K. As $\mathrm{Gal}(f)$ is trivial, we can repeatedly apply Theorem 12.3 (and Lemma 11.21) to the given C2D4 structure $C^{(1)}$ to change it to the standard C2D4 structure $C^{(0)} \in \mathcal{F}_{C2D4}$. Conjecture 1.14 holds for $C^{(0)}$ (Theorem 10.5), and hence for $C^{(1)}$ as well. □

12.5 | Changing the isogeny (continued)

Proof of Theorem 12.3 for K archimedean or a finite extension of $\mathbb{Q}_p$, p odd. Let F be a number field with a prime v such that $F_v \simeq K$ and F has a complex place $v' \neq v$. By Theorem 12.4, Conjecture 1.14 holds for all curves over 2-adic fields that lie in $\mathcal{F}$, irrespectively of the choice of the C2D4 structure. The proof now follows verbatim as the third paragraph of the proof of the case when K is an extension of $\mathbb{Q}_2$. □

12.6 | Proof of Theorem 1.16

Theorem 12.5 (=Theorem 1.16). *Conjecture 1.14 holds for all C2D4 curves with $\mathcal{P}, \Delta \neq 0$ over archimedean local fields, all semistable C2D4 curves with $\mathcal{P}, \Delta \neq 0$ over finite extensions of $\mathbb{Q}_p$ for odd primes p and all C2D4 curves with $\mathcal{P}, \Delta \neq 0$ and good ordinary reduction over finite extensions of $\mathbb{Q}_2$.*

Proof. Write the curve as $C : y^2 = cf(x)$ and consider the colouring of the roots of $f(x)$ given by the C2D4 structure, $C^{(1)}$. Observe that

(1) if $\mathrm{Gal}(f)$ preserves colours, then C admits two other C2D4 structures obtained from the original one by relabelling the colours; and
(2) if $\mathrm{Gal}(f)$ acts as a subgroup of V_4 on the sapphire and turquoise roots, then C admits two other C2D4 structures obtained from the original one by changing the colouring of sapphire and turquoise roots.

Let $C^{(2)}$ be any one of these structures. By Lemma 11.21, we may assume that $C^{(2)}$ also has $\mathcal{P}, \Delta \neq 0$. By Theorem 12.3, it then suffices to prove the result for $C^{(2)}$.

We now show that through repeated use of (1) and (2), we can reduce the problem to one already covered by Theorems 4.1 and 12.2.

Complex places: The result is covered by Theorem 4.1.

Real places: We may assume that if $f(x)$ has a real root, then $c < 0$: indeed, by Theorem 12.1, we can use a change of model given by $x \mapsto \frac{1}{x-t}$ for a suitable $t \in \mathbb{R}$ to make the leading term negative.

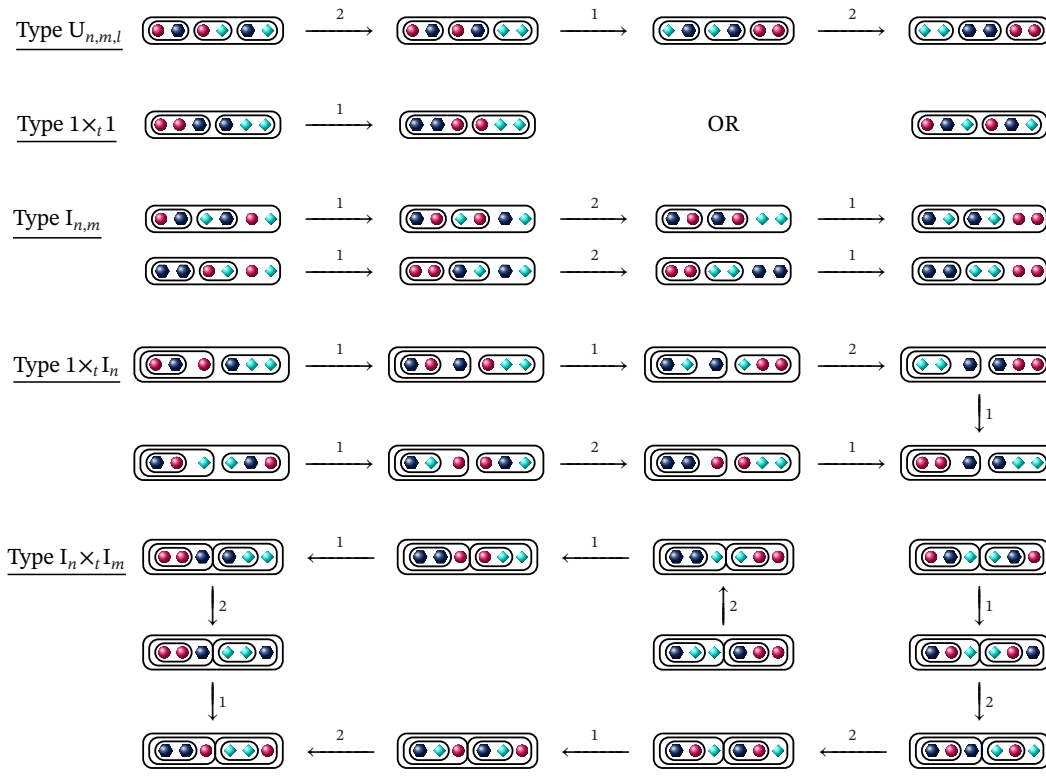
If $f(x)$ has six real roots, then a repeated use of (1) and (2) brings it to the picture  .

If $f(x)$ has four real roots, then by (1), we may assume that the complex roots are ruby, and then, by (2) that the picture is  with $\alpha_1 = \bar{\beta}_1$.

If $f(x)$ has two real roots, then by (1), we may assume that these are ruby, and then by (2) that the picture is  with $\alpha_2 = \bar{\beta}_2$ and $\alpha_3 = \bar{\beta}_3$, and then by (1) again that the picture is instead with $\alpha_1 = \bar{\beta}_1$ and $\alpha_3 = \bar{\beta}_3$.

If $f(x)$ has no real roots, then the ruby roots are necessarily complex conjugate, and by (2), we can make $\alpha_i = \bar{\beta}_i$ for $i = 1, 2, 3$.

Odd primes: By Theorems 6.5 and 12.1, we may assume that the cluster picture of C/K is balanced (using Lemma 3.7(5) to enlarge $|k|$ if necessary). If the reduction has type 2 or 1_n (in the sense of Theorem 2.17), the result follows from Theorem 12.2. Otherwise, its cluster picture is one of the ones given below. Applying steps (1) and (2) as indicated above the arrows reduces the problem to one covered by Theorem 12.2.



2-adic primes: By Proposition 10.2(i) and Theorem 12.1, we may assume that the cluster picture of C has three twins of depth $v(4)$, and that the depth of the cluster containing all six roots is 0 (using Lemma 3.7(5) to first enlarge $|k|$ if necessary). The result follows as for the case of Type $U_{n,m,l}$ above. □

13 | GLOBAL RESULTS

We now complete the proofs of the theorems given in the introduction.

Proposition 13.1. *The 2-parity conjecture holds for abelian varieties over number fields A/K with* $\mathrm{Gal}(K(A[2])/K)$ *a 2-group that are either products of elliptic curves, or the Weil restriction of an elliptic curve from a field extension.*

Proof. If $A \simeq \prod E_i$ or $\simeq \mathrm{Res}_{F/K} E$, then the condition on the 2-torsion field ensures that the elliptic curves E_i/K or E/F all admit a 2-isogeny. By [13, Thm. 5.8], the 2-parity conjecture holds for E_i/K (respectively, E/F). As the 2-parity conjecture is compatible with products and with Weil restriction of scalars (as both root numbers and p^∞-Selmer ranks are), it also holds for A/K. □

Theorem 13.2. *The 2-parity conjecture holds for all C2D4 curves over number fields C/K with* $\Delta = 0$.

Proof. By [31, Def. 8.2.4 and Prop. 8.3.1], $A = \operatorname{Jac} C$ has an isogeny of degree 4 to an abelian variety B that is either a product of two elliptic curves or the Weil restriction of an elliptic curve from a quadratic extension. By hypothesis, $\mathrm{Gal}(K(A[2])/K)$ is a 2-group, and hence so is $\mathrm{Gal}(K(A[2^n])/K)$. It follows that $\mathrm{Gal}(K(B[2])/K)$ is also a 2-group. The result now follows by Proposition 13.1, since the 2-parity conjecture is compatible with isogenies (as both root numbers and p^∞-Selmer ranks are invariant under isogenies). □

Theorem 13.3. *The 2-parity conjecture holds for all principally polarised abelian surfaces over number fields A/K such that* $\mathrm{Gal}(K(A[2])/K)$ *is a 2-group that are either*

- *the Jacobian of a semistable genus 2 curve with good ordinary reduction at primes above 2, or*
- *not isomorphic to the Jacobian of a genus 2 curve.*

Proof. By [17, Thm. 3.1], A is either a product of two elliptic curves, the Weil restriction of an elliptic curve from a quadratic field extension or is the Jacobian of a genus 2 curve C/K. By Proposition 13.1 and the hypothesis on the 2-torsion field, we may assume that $A = \operatorname{Jac} C$ for a C2D4 curve C/K. By Theorem 13.2 and Lemma 11.17, we may also assume that $\mathcal{P}, \Delta \neq 0$. The result now follows from Theorems 1.15 and 12.5. □

Corollary 13.4. *The 2-parity conjecture holds for all semistable C2D4 curves over number fields C/K that have good ordinary reduction at the primes above 2.*

Theorem 13.5. *The parity conjecture holds for all principally polarised abelian surfaces over number fields A/K such that* $Ш_{A/K(A[2])}$ *has finite 2-, 3- and 5-primary part that are either*

- *the Jacobian of a semistable genus 2 curve with good ordinary reduction at primes above 2, or*
- *semistable, and not isomorphic to the Jacobian of a genus 2 curve.*

Proof. This now follows from Theorems 13.3 and B.1. □

Theorem 13.6. *If the 2-parity conjecture is true for all Jacobians of C2D4 curves over number fields, then Conjecture 1.14 holds for all C2D4 curves over local fields of characteristic 0 with $\mathcal{P}, \Delta \neq 0$.*

Proof. Let C/K be a C2D4 curve over a local field of characteristic 0 with $\mathcal{P} \neq 0$. Let F be a number field with a place v, such that $F_v \cong K$, and some other place v' that is archimedean.

By Lemma 11.19, we may assume that $\eta_1 \neq 0$. By Theorems 11.15 and 12.5, we can find a C2D4 curve C' over F such that C and C' are arithmetically close over F_v and such that Conjecture 1.14 holds for C/F_w for all places $w \neq v$. By assumption, the 2-parity conjecture holds for C'/F, so by Lemma 1.19, Conjecture 1.14 holds for C/F_v. It follows by Lemma 11.4 that Conjecture 1.14 also holds for C/K. □

APPENDIX A: ISOGENIES BETWEEN ABELIAN VARIETIES WITH GOOD ORDINARY REDUCTION by Adam Morgan

A.1 | Statement of the result

Let K be a finite extension of $\mathbb{Q}_2$ and A/K a principally polarised abelian variety of dimension g, with good ordinary reduction. Let W be a maximal isotropic subspace of $A[2]$ (for the Weil

pairing associated to the principal polarisation), stable under the action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. Let $\phi : A \to B$ be the K-isogeny with kernel W, so that B is principally polarised also, has good ordinary reduction, and (after identifying A and B with their duals) the dual isogeny $\hat{\phi} : B \to A$ satisfies

$$\phi \circ \hat{\phi} = \hat{\phi} \circ \phi = [2].$$

Let $A_1(\bar{K})$ denote the kernel of reduction on A.

The aim of the Appendix is to prove the following result, whose proof we give in §A.3 after reviewing endomorphisms of the formal multiplicative group.

Theorem A.1. *With the notation above we have*

$$\frac{|B(K)/\phi(A(K))|}{|A(K)[\phi]|} = 2^{[K:\mathbb{Q}_2]\dim_{\mathbb{F}_2}(A_1(\bar{K})[2] \cap A(\bar{K})[\phi])}.$$

A.2 | Endomorphisms of the formal multiplicative group

Again, let K be a finite extension of $\mathbb{Q}_2$, and let T denote the completion of the maximal unramified extension of K. Let $\mathcal{O}$ be the ring of integers of T, so that $\mathcal{O}$ is a complete discrete valuation ring, whose normalised valuation restricts to that of K. Let $\widehat{\mathbb{G}}_m$ denote the formal multiplicative group over $\mathcal{O}$. In general, given formal group laws $\mathcal{F}$ and $\mathcal{G}$ over $\mathcal{O}$ of dimension g, and a homomorphism ϕ from $\mathcal{F}$ to $\mathcal{G}$, we denote by $D(\phi)$ the *Jacobian* of ϕ. That is, ϕ is an n-tuple of power series in g variables $X = (x_1, \dots, x_g)$, coefficients in $\mathcal{O}$, and $D(\phi) \in \mathrm{M}_g(\mathcal{O})$ is an $g \times g$ matrix such that

$$\phi(X) \equiv D(\phi)X \pmod{\deg 2}.$$

The homomorphism ϕ is an isomorphism if and only if $D(\phi)$ is invertible in $\mathrm{M}_g(\mathcal{O})$.

Lemma A.2. *For each $g \geqslant 1$, the map $\phi \mapsto D(\phi)$ gives an isomorphism of rings*

$$End_{\mathcal{O}}(\widehat{\mathbb{G}}_m^g) \xrightarrow{\sim} \mathrm{M}_g(\mathbb{Z}_2).$$

Proof. The result for general g follows formally from the case $g = 1$, which is standard, although we provide the proof for convenience. The formal logarithm gives an isomorphism from $\widehat{\mathbb{G}}_m$ to the formal additive group $\widehat{\mathbb{G}}_a$ over T, and the endomorphisms of the latter are given by $\phi(X) = aX$ for $a \in T$. Thus, one sees that the endomorphisms of $\widehat{\mathbb{G}}_m$ over $\mathcal{O}$ are exactly those of the form

$$\phi_a(X) = aX + a(a-1)X^2/2 + a(a-1)(a-2)x^3/3! + \cdots$$

for those $a \in T$ such that each coefficient of $\phi_a(X)$ is in $\mathcal{O}$. Considering the coefficients of x^{2^n} for varying n, one sees easily that this is equivalent to $a \in \mathbb{Z}_2$, from which the result follows. □

Now let $\mathfrak{m}$ denote the maximal ideal in $\mathcal{O}$. Letting $U^1(T)$ denote the group of units in $\mathcal{O}$ reducing to 1 in the residue field $\mathcal{O}/\mathfrak{m}$, the map

$$(x_1, \dots, x_g) \mapsto (x_1 - 1, \dots, x_g - 1)$$

gives an isomorphism from $U^1(T)^g$ to $\mathfrak{m}^g$ with the group structure on the latter coming from the formal group law $\widehat{\mathbb{G}}_m^g$. Any endomorphism $\phi \in \mathrm{End}_{\mathcal{O}}(\widehat{\mathbb{G}}_m^g)$ induces via this isomorphism an endomorphism of $U^1(T)^g$. We denote by $U^1(T)^g[\phi]$ the kernel of this map.

Lemma A.3. *Let $\phi \in \mathrm{End}_{\mathcal{O}}(\widehat{\mathbb{G}}_m^g)$ and suppose that there is $\psi \in \mathrm{End}_{\mathcal{O}}(\widehat{\mathbb{G}}_m^g)$ such that $\phi\circ\psi = [2]$ (here [2] denotes the multiplication-by-2 map on $\widehat{\mathbb{G}}_m^g$). Then $U^1(T)^g[\phi]$, being contained in $U^1(T)^g[2] = \{\pm 1\}^g$, is a finite-dimensional $\mathbb{F}_2$-vector space and we have*

$$\dim_{\mathbb{F}_2} U^1(T)^g[\phi] = \mathrm{ord}_2 \det D(\phi).$$

Proof. Let $M = D(\phi) \in M_g(\mathbb{Z}_2)$. By properties of Smith Normal Form, we can find invertible matrices V and W in $M_g(\mathbb{Z}_2)$ such that $M = VNW$ where N is a diagonal matrix whose entries are powers of 2. On the other hand, $D(\phi)D(\psi)$ is twice the identity matrix. Thus,

$$2V^{-1} = NWD(\psi).$$

In particular, each coefficient of $NWD(\psi)$ is divisible by 2, yet $\frac{1}{2}NWD(\psi)$ has determinant a 2-adic unit. If one of the entries of N was divisible by 4, then 2 would divide each entry of some row of $\frac{1}{2}NWD(\psi)$, and hence its determinant, a contradiction. We deduce that each entry of N is either 1 or 2. Moreover, the matrices V and W correspond to automorphisms of $\widehat{\mathbb{G}}_m^g$ under Lemma A.2 and since we are only interested in the size of the kernel of ϕ, we may replace ϕ with the endomorphism corresponding to N (by construction, we also have $\mathrm{ord}_2 \det D(\phi) = \mathrm{ord}_2 \det N$). However, as N is diagonal with entries either 1 or 2, the endomorphism of $U^1(T)^g$ induced by N is just the identity on each factor where N has a 1 on the diagonal, and the map $x \mapsto x^2$ on each factor where N has a 2 on the diagonal. The $\mathbb{F}_2$-dimension of the kernel of this map is just the number of diagonal entries of N equal to 2, which is equal to $\mathrm{ord}_2 \det N$. □

A.3 | Proof of Theorem A.1

We keep the notation of §A.1 and §A.2, so that, in particular, let A/K be a principally polarised abelian variety of dimension g with good ordinary reduction, let B/K be isogenous to A via ϕ, and consider the auxiliary isogeny $\psi : B \to A$ such that $\phi\circ\psi = [2]$. Let v_T be the normalised valuation on T (which extends that on K), k denote the residue field of K, and let $e(K/\mathbb{Q}_2)$ be the ramification index of K over $\mathbb{Q}_2$. Let $\mathcal{F}_A$ and $\mathcal{F}_B$ be the dimension g formal group laws over the ring of integers $\mathcal{O}_K$ of K associated to A and B, respectively. Then ϕ induces an element of $\mathrm{Hom}_{\mathcal{O}_K}(\mathcal{F}_A, \mathcal{F}_B)$ which, by an abuse of notation, we also denote by ϕ. Similarly, we obtain $\psi \in \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{F}_B, \mathcal{F}_A)$ and we have $\phi\circ\psi = [2]$. Since A and B have good ordinary reduction, over $\mathcal{O}$ (the ring of integers of T), there is an isomorphism α from $\mathcal{F}_A$ to $\widehat{\mathbb{G}}_m^g$, and similarly an isomorphism β from $\mathcal{F}_B$ to $\widehat{\mathbb{G}}_m^g$ (see [24, Lemma 4.27] for more details). We thus obtain elements $\phi' := \beta\phi\alpha^{-1}$ and $\psi' := \alpha\psi\beta^{-1}$ of $\mathrm{End}_{\mathcal{O}}(\widehat{\mathbb{G}}_m^g)$ whose composition is multiplication by 2. Moreover, since α and β are isomorphisms, $D(\alpha)$ and $D(\beta)$ are invertible matrices in $M_n(\mathcal{O})$. In particular, the determinants of $D(\alpha)$ and $D(\beta)$ are units in $\mathcal{O}$. Thus,

$$v_K(\det D(\phi)) = v_T(\det D(\phi')) = e(K/\mathbb{Q}_2)\,\mathrm{ord}_2 \det D(\phi').$$

Applying Lemma A.3, we obtain

$$v_K(\det D(\phi)) = e(K/\mathbb{Q}_2)\dim_{\mathbb{F}_2} U^1(T)^g[\phi'].$$

Let $\bar{K}$ be an algebraic closure of K and let $A_1(\bar{K})[2]$ denote the points in $A(\bar{K})[2]$ reducing to the identity under the reduction map into $\bar{k}$ (the algebraic closure of k). Then since A has good ordinary reduction, $A_1(\bar{K})[2]$ has size 2^g. On the other hand, the points in $A_1(T)$ correspond

isomorphically under α to the points of $U^1(T)^g$, and there are 2^g such 2-torsion points in this latter group, namely the points $\{\pm 1\}^g$. In particular, we deduce that

$$\dim_{\mathbb{F}_2} U^1(T)[\phi'] = \dim_{\mathbb{F}_2} (A_1(\bar{K})[2] \cap A(\bar{K})[\phi]).$$

We thus have

$$\operatorname{ord}_2\left(|\det D(\phi)|_K^{-1}\right) = [K : \mathbb{Q}_2] \dim_{\mathbb{F}_2} (A_1(\bar{K})[2] \cap A(\bar{K})[\phi]).$$

On the other hand, since the Néron component groups of A and B are both trivial, the left-hand side of the above equality is equal to

$$\operatorname{ord}_2 \frac{\left|B(K)/\phi(A(K))\right|}{\left|A(K)[\phi]\right|},$$

as follows from [29, Lemma 3.8].

APPENDIX B: PARITY REDUCTION TO 2-SYLOW
by T. Dokchitser and V. Dokchitser

Recall that the parity conjecture (Conjecture 1.1) relates the parity of the Mordell–Weil rank of a principally polarised abelian variety A over a number field K to the global root number,

$$(-1)^{\operatorname{rk} A/K} = w(A/K).$$

In this appendix, we show that, assuming finiteness of Ш (and a mild restriction on the reduction of A), the conjecture follows from its special case when A admits a suitable 2-power isogeny. This special case was proved for elliptic curves in [10] and this reduction approach was proved in [12] to deduce the general case for elliptic curves. The present article deals with the case of abelian surfaces. Ironically, [8] establishes the analogous result for a p-power isogeny when p is odd.

Theorem B.1. *Let F/K be a Galois extension of number fields with Galois group G, and A/K a principally polarised abelian variety. Suppose*

(1) *Ш(A/F) has finite p-primary part for every odd prime p that divides $|G|$,*
(2) *all primes of unstable reduction of A have cyclic decomposition groups in G.*

If the parity conjecture holds for A/F^H for all $H \leqslant G$ of 2-power order, then it holds for A/K.

Corollary B.2. *Let K be a number field, A/K a principally polarised abelian variety, and write $F = K(A[2])$. Suppose that*

(1) *Ш(A/F) has finite p-primary part for every odd prime $p \mid [F : K]$,*
(2) *all primes of unstable reduction of A have cyclic decomposition groups in F/K,*
(3) *the parity conjecture holds for A/L for subfields $K \subset L \subset F$ over which A admits an isogeny $\phi : A \to A'$ with $\phi\phi^t = [2]$.*

Then the parity conjecture holds for A/K.

Note the assumption (2) in B.1 and B.2 holds when A/K is semistable. We now turn to the proofs.

Lemma B.3. *Let G be a finite group. Then*

$$\mathbf{1}_G = \sum n_i \operatorname{Ind}_{H_i}^G \mathbf{1}_{H_i}$$

for some $n_i \in \mathbb{Z}$, and where each H_i is one of the following types of subgroups of G:

(1) *H_i has 2-power order; or*
(2) *there is $U \lhd H$ with $H/U \cong C_p \rtimes C_{2^k}$ for p an odd prime, $k \geqslant 0$, and C_{2^k} acting faithfully on C_p.*

Proof. We proceed by induction on $|G|$. Solomon's induction theorem expresses $\mathbf{1}_G$ as an integral linear combination of $\operatorname{Ind}_{H_i}^G \mathbf{1}_{H_i}$ for some hyperelementary $H_i < G$. As induction is transitive, we may assume that G is hyperelementary. (Recall that a group G is hyperelementary if $G \simeq C \rtimes P$ for a p-group P and a cyclic group C of order prime to p.)

If G has a non-trivial odd order quotient, then it has a C_p-quotient for some odd prime p, and we are done by (2). Otherwise, $G = C_n \rtimes P$ for some odd n and a 2-group P. If $n = 1$, we are done by (1). By passing to a quotient if necessary, we may assume that n is prime and, moreover, that P acts faithfully. Then we are done by (2). □

Recall that for a prime l, we define the dual l^∞-Selmer group,

$$X_l(A/K) = (\text{Pontryagin dual of the } l^\infty\text{-Selmer group of } A/K) \otimes \mathbb{Q}_l.$$

This is a $\mathbb{Q}_l$-vector space whose dimension is the Mordell–Weil rank of A/K plus the number of copies of $\mathbb{Q}_l/\mathbb{Z}_l$ in Ш(A/K).

Conjecture B.4 (l-Parity conjecture = Conjecture 1.4).

$$(-1)^{\dim X_l(A/K)} = w(A/K).$$

If Ш is finite, this is equivalent to the parity conjecture.

Lemma B.5. *Let F/K be a Galois extension of number fields with Galois group $G = C_p \rtimes C_{2^k}$ with p an odd prime, $k \geqslant 0$, and C_{2^k} acting faithfully on C_p. Let A/K be a principally polarised abelian variety and l a prime. Suppose either*

(1) *$k = 0$; or*
(2) *$0 < k < \operatorname{ord}_2(p-1)$, and either $l = p$ or the 2-part of the order of $l \in \mathbb{F}_p^\times$ is $> k$; or*
(3) *$k = \operatorname{ord}_2(p-1)$, $l = p$ and all primes of unstable reduction of A have cyclic decomposition groups in G.*

If the l-parity conjecture holds for A/L for all $K \subsetneq L \subset F$, then it holds for A/K.

Proof.

(1) l-parity is invariant under odd degree Galois extensions, see, for example, [11, Cor. A.3(3)].
(2) The (absolutely) irreducible representations of G are 1-dimensionals that factor through C_{2^k} and 2^k-dimensionals of the form $\rho_\psi = \operatorname{Ind}_{C_p}^G \psi$ for faithful 1-dimensional ψ. The field generated by the character of ψ is $\mathbb{Q}(\zeta_p)$, so the number of $\operatorname{Gal}(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$-conjugates of ψ is $[\mathbb{Q}_l(\zeta_p) : \mathbb{Q}_l]$, which is the order of l in $\mathbb{F}_p^\times$. In particular, under the assumption on l, ρ_ψ has an

even number of images under $\mathrm{Gal}(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$, so that each irreducible $\mathbb{Q}_l$-representation has an even number of absolutely irreducible constituents. Thus,

$$\mathrm{rk}_l\, A/F^{C_{2^k}} = \dim X_l^{C_{2^k}} = \langle X_l, \mathrm{Ind}_{C_{2^k}}^G \mathbf{1}\rangle = \langle X_l, \mathbf{1} \oplus \bigoplus_{\rho_\psi} \rho_\psi\rangle$$

$$\equiv \langle X_l, \mathbf{1}\rangle = \mathrm{rk}_l\, A/K \bmod 2,$$

where the direct sum ranges over absolutely irreducible non-one-dimensional representations of G. Also, by [28, Thm. 1] (or [11, Prop. A.2(5)]), twists of A by Galois conjugate orthogonal characters have the same root number, so $w(A,\rho_\psi) = w(A,\rho'_\psi)$ for all $\psi, \psi' \neq \mathbf{1}$, and

$$w(A/F^{C_{2^k}}) = w(A, \mathbf{1} \oplus \bigoplus_{\rho_\psi} \rho_\psi) = w(A/K).$$

Therefore, l-parity over $F^{C_{2^k}}$ implies l-parity over K, as claimed.

(3) We invoke the regulator constant machinery of [11, 12] that proves special cases of the parity conjecture by exploiting Brauer relations in Galois groups. There is a Brauer relation in G (see, e.g. [1, Ex. 2.3])

$$\Theta = C_1 - C_p - 2^k C_{2^k} + 2^k G.$$

Write ϵ for the order 2 character of C_{2^k}, and ψ_i for its other non-trivial characters. Then the irreducible self-dual $\mathbb{Q}_p G$-representations are $\mathbf{1}, \epsilon, \psi_i \oplus \psi_i^{-1}$ and $\rho = \mathrm{Ind}_{C_{2^k}}^G \ominus \mathbf{1}$. The regulator constants (over $\mathbb{Q}_p$) $C_\Theta(\psi_i \oplus \psi_i^{-1})$ are 1 by [11, Cor. 2.25(3)]. We can compute the others using, for example, [11, Ex. 2.19], and we find

$$C_\Theta(\mathbf{1}) = C_\Theta(\epsilon) = C_\Theta(\rho) = p.$$

(This is done in [11, Ex. 2.20] when $k = 1$.)

By [11, Thm. 1.6b], the l-parity conjecture holds for the twist of A/K by any self-dual $\bar{\mathbb{Q}}_p G$-representation τ such that

$$\langle \tau, \mathbf{1}\rangle = \langle \tau, \epsilon\rangle = \langle \tau, \rho\rangle \equiv 1 \bmod 2.$$

Since $\langle \rho, \rho\rangle = \frac{p-1}{2^k}$ is odd, we can take

$$\tau = \mathrm{Ind}_{C_{2^k}}^G \mathbf{1} + \mathrm{Ind}_{C_p}^G \mathbf{1} + \mathbf{1}.$$

Since l-parity holds over $F^{C_{2^k}}$ and over F^{C_p} by assumption, it holds for the twists of A by $\mathrm{Ind}_{C_{2^k}}^G \mathbf{1}$ and by $\mathrm{Ind}_{C_p}^G \mathbf{1}$ (see [11, Cor. A.3(2)]), and therefore, for A/K. □

Proof of Theorem B.1. We proceed by induction on $|G|$. Write $\mathbf{1} = \sum n_i \mathrm{Ind}_{H_i}^G \mathbf{1}$ as in Lemma B.3. Then

$$\mathrm{rk}\, A/K = \langle A(F)\otimes_{\mathbb{Z}} \mathbb{C}, \mathbf{1}\rangle = \sum_i \langle A(F)\otimes_{\mathbb{Z}} \mathbb{C}, n_i \mathrm{Ind}_{H_i}^G \mathbf{1}\rangle$$

$$= \sum_i n_i \langle A(F)\otimes_{\mathbb{Z}} \mathbb{C}, \mathbf{1}\rangle_{H_i} = \sum_i n_i\, \mathrm{rk}\, A/F^{H_i}.$$

Similarly, by Artin formalism for root numbers,

$$w(A/K) = \prod_i w(A/F^{H_i})^{n_i}.$$

Therefore, it suffices to prove parity for A/F^{H_i} for all i. If H_i has 2-power order, then parity holds by assumption. If H_i is as in Lemma B.3(2), it holds by Lemma B.5 and the inductive hypothesis, noting that the assumptions (1) and (2) hold in all intermediate Galois extensions F'/K' inside F/K; for (1), see, for example, [12, Remark 2.10]. □

Lemma B.6. *Let V be a symplectic $\mathbb{F}_2$-vector space of dimension $2n$. Then the 2-Sylow subgroup H of $\mathrm{Sp}(V)$ stabilises an n-dimensional totally isotropic subspace.*

Proof. We construct a totally isotropic H-invariant subspace W_m of dimension m for $0 \leqslant m \leqslant n$ by induction. Take $W_0 = \{0\}$. For $m > 0$, let $X = \frac{W_{m-1}^{\perp}}{W_{m-1}} \setminus \{0\}$, pick an H-invariant vector $v \in X$ and set W_m to be the span of W_{m-1} and any lift of v to V. Such a v exists because $X \neq \emptyset$ (as $m \leqslant n$), and a 2-group acting on a set of odd order has a fixed point. □

Proof of Theorem B.2. Write $G = \mathrm{Gal}(F/K)$. Suppose $H < G$ has 2-power order. By the above lemma, $A[2]$ has an H-invariant totally isotropic subspace. It is a standard fact that A/F^H therefore admits an isogeny $\phi : A \to A'$ with $\phi\phi^t = [2]$. By hypothesis, the parity conjecture holds for A/F^H. The result follows by Theorem B.1. □

ACKNOWLEDGEMENTS

We would like to warmly thank Tim Dokchitser and Adam Morgan for contributing the appendices, numerous helpful discussions and for undertaking our joint project [15], which was essential for the present article. We are very grateful to the anonymous referee for their exceptionally detailed report and their suggestions for improvements. We would like to thank Andrew Sutherland for providing useful data on genus 2 curves over 2-adic fields. We also thank the University of Warwick, King's College London, Boston University, Max Planck Institute and the University of Bristol, where parts of this work were carried out. The first author was supported by a Royal Society University Research Fellowship. This research was partially supported by EPSRC grants EP/M016838/1 and EP/M016846/1 'Arithmetic of hyperelliptic curves' and the Simons Collaboration grant 550023 'Arithmetic Geometry, Number Theory, and Computation'.

JOURNAL INFORMATION

The *Proceedings of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

REFERENCES

1. A. Bartel and T. Dokchitser, *Brauer relations in finite groups*, J. Eur. Math. Soc. **17** (2015), 2473–2512.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I: The user language*, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.
3. N. Bruin and K. Doerksen, *The arithmetic of genus 2 curves with (4,4)-split Jacobians*, Canada J. Math. **63** (2011), no. 5.

4. A. Betts and V. Dokchitser, *Variation of Tamagawa numbers of semistable abelian varieties in field extensions*, Math. Proc. Cambridge Philos. Soc. **166** (2019), no. 3, 487–521.
5. S. Bosch and D. Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), 353–396.
6. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow arithmetic of curves of genus 2*, London Mathematical Society, Lecture Note Series, vol. 230, Cambridge University Press, Cambridge, 1996.
7. K. Cesnavicius, *The ℓ-parity conjecture over the constant quadratic extension*, Math. Proc. Cambridge Philos. Soc. **165** (2018), no. 3, 385–409.
8. J. Coates, T. Fukaya, K. Kato, and R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Algebriac Geom. **19** (2010), 19–97.
9. J. Docking, *2^∞-Selmer rank parities via the Prym construction*, arxiv: 2108.09564.
10. T. Dokchitser and V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), 662–679.
11. T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71.
12. T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. **172** (2010), no. 1, 567–596.
13. T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39–64.
14. T. Dokchitser and V. Dokchitser, *Local invariants of isogenous elliptic curves*, Trans. Amer. Math. Soc. **367** (2015), 4339–4358.
15. T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), no. 3–4, 1213–1322.
16. V. Dokchitser and A. Morgan, *A note on hyperelliptic curves with ordinary reduction over 2-adic fields*, J. Number Theory **244** (2023), 264–278.
17. J. Gonzáles, J. Guàrdia, and V. Rotger, *Abelian surfaces of GL2-type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287.
18. B. Gross and J. Harris, *Real algebraic curves*, Ann. Sci. Éc. Norm. Supér. **14** (1981), no. 2, 157–182.
19. A. Grothendieck, *Groupes de monodromie en Géométrie Algébrique SGA 7, I*, LNM, vol. 288, Springer, Berlin, Heidelberg, 1972.
20. E. Halberstadt, *Signes locaux des courbes elliptiques en 2 et 3*, C. R. Acad. Sci. Paris Ser. I Math. **326** (1998), no. 9, 1047–1052.
21. M. Kisin, *Local constancy in p-adic families of Galois representations*, Math. Z. **230** (1999), 569–593.
22. Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. AMS **348** (1996), no. 11, 4577–4610.
23. C. Maistret, *Parity of ranks of Jacobians of hyperelliptic curves of genus 2*, Ph.D. thesis, University of Warwick, http://wrap.warwick.ac.uk/93324.
24. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
25. J. S. Milne, *Jacobian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 167–212.
26. A. Morgan, *2-Selmer parity for hyperelliptic curves in quadratic extensions*, arxiv:1504.01960.
27. B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. **150** (1999), 1109–1149.
28. D. Rohrlich, *Galois invariance of local root numbers*, Math. Ann. **351** (2011), no. 4, 979–1003.
29. E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), 79–114.
30. J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, Series, vol. 7, Springer, New York, NY, 1973.
31. B. Smith, *Explicit endomorphisms and Correspondence*, Ph.D. thesis, 2005.
32. R. van Bommel, *Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over $\mathbb{Q}$ up to squares*, Exp. Math. **31** (2022), no. 1.