RESEARCH ARTICLE

2-Selmer parity for hyperelliptic curves in quadratic extensions

Adam Morgan ⬤

School of Mathematics and Statistics,
University of Glasgow, University Place,
Glasgow, UK

Correspondence
Adam Morgan, School of Mathematics
and Statistics, University of Glasgow,
University Place, Glasgow, G12 8QQ, UK.
Email: ajmorgan44@gmail.com

Abstract

We study the 2-parity conjecture for Jacobians of hyperelliptic curves over number fields. Under some mild assumptions on their reduction, we prove the conjecture over quadratic extensions of the base field. The proof proceeds via a generalisation of a formula of Kramer and Tunnell relating local invariants of the curve, which may be of independent interest. A new feature of this generalisation is the appearance of terms which govern whether or not the Cassels–Tate pairing on the Jacobian is alternating, which first appeared in work of Poonen–Stoll. We establish the local formula in many instances and show that in remaining cases, it follows from standard global conjectures.

MSC 2020
11G40 (primary), 11G10, 11G20, 11G30, 14G10, 14K15 (secondary)

Contents

1 │ INTRODUCTION

Let K be a number field and A/K an abelian variety. Conjecturally, the corresponding completed L-function of A/K, $L^\star(A/K, s)$, has an analytic continuation to the whole of the complex plane and satisfies a functional equation

$$L^\star(A/K, s) = w(A/K)L^\star(A/K, 2 - s),$$

where $w(A/K) \in \{\pm 1\}$ is the global root number of A/K. The Birch and Swinnerton-Dyer conjecture asserts that the Mordell–Weil rank of A/K agrees with the order of vanishing at $s = 1$ of $L^\star(A/K, s)$:

$$\mathrm{ord}_{s=1} L^\star(A/K, s) = \mathrm{rk}(A/K).$$

If $w(A/K) = 1$ (resp. -1), then $L^\star(A/K, s)$ is an even (resp. odd) function around $s = 1$ and as such its order of vanishing there is even (resp. odd). Thus, a consequence of the Birch and Swinnerton-Dyer conjecture is the parity conjecture:

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

Essentially, all progress towards the parity conjecture has proceeded via the p-parity conjecture. For a fixed prime p, denote by $\mathrm{rk}_p(A/K)$ the p-infinity Selmer rank of A/K. Under the conjectural finiteness of the Shafarevich–Tate group (or indeed, under the weaker assumption that its p-primary part is finite), $\mathrm{rk}_p(A/K)$ agrees with $\mathrm{rk}(A/K)$. The p-parity conjecture is the assertion that

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

Note that without knowing finiteness of the Shafarevich–Tate group, these conjectures are inequivalent for different primes p.

1.1 │ Known cases of the *p*-parity conjecture

For elliptic curves over $\mathbb{Q}$, Dokchitser–Dokchitser [16] have shown that the p-parity conjecture holds for all primes p. Subsequently, Nekovář [44] extended this result to all totally real number

fields, excluding some elliptic curves with potential complex multiplication; these exceptional cases have recently been treated by Green–Maistret [22]. For a general number field K, Česnavičius [8] has shown that the p-parity conjecture holds for elliptic curves over K possessing a p-isogeny, whilst work of Kramer–Tunnell [27] and Dokchitser–Dokchitser [17] proves that the 2-parity conjecture holds for an arbitrary elliptic curve E/K, not over K itself, but over any quadratic extension of K.

For higher dimensional abelian varieties, much less is known. The most general result at present is due to Coates, Fukaya, Kato and Sujatha, who prove in [11] that for odd primes p, the p-parity conjecture holds for any abelian variety possessing a suitable p-power degree isogeny, subject to some further technical conditions. For $p = 2$, the main result is due to Dokchitser–Maistret [19], who prove the 2-parity conjecture for quite general semistable abelian surfaces.

1.2 | Main result

Following on from the work of Kramer–Tunnell and Dokchitser–Dokchitser for elliptic curves, we consider the 2-parity conjecture for Jacobians of hyperelliptic curves over quadratic extensions of their field of definition. Our main result is the following.

Theorem 1.1. *Let K be a number field and L/K a quadratic extension. Let C/K be a hyperelliptic curve of genus $g \geqslant 2$ and let J/K be the Jacobian of C. Suppose that J has semistable reduction at each prime $\mathfrak{p} \nmid 2$ of K which ramifies in L/K, and assume moreover that:*

- *for each prime $\mathfrak{p} \mid 2$ of K which is inert in L/K, J has good reduction at $\mathfrak{p}$,*
- *for each prime $\mathfrak{p} \mid 2$ of K which ramifies in L/K, J has good ordinary reduction at $\mathfrak{p}$ and $K_{\mathfrak{p}}(J[2])/K_{\mathfrak{p}}$ has odd degree.*

Then the 2-parity conjecture holds for J/L.

Remark 1.2. Theorem 1.1 gives a large supply of hyperelliptic curves satisfying the 2-parity conjecture over every quadratic extension of their field of definition; see Lemma 16.5 for explicit conditions on a Weierstrass equation defining C that ensure that the conditions of Theorem 1.1 at primes dividing 2 are satisfied.

Remark 1.3. If the genus of C is 2, then one can weaken the assumption that J has good reduction at each inert prime dividing 2 to assume only that J has semistable reduction at such primes; see Proposition 9.1.

1.3 | Reduction to a local question

The proof of Theorem 1.1 proceeds by reducing to a purely local question, as we now explain.

In the notation of Theorem 1.1, for each place v of K which is non-split in L, denote by $\mathfrak{v}$ the unique place of L extending v. Since J is defined over K, the root number $w(J/L)$ decomposes as

a product of local terms indexed by places of K which are non-split in L/K:

$$w(J/L) = \prod_{\substack{v \text{ place of } K \\ v \text{ non-split in } L}} w(J/L_{\mathfrak{v}}), \tag{1.4}$$

where $w(J/L_{\mathfrak{v}}) \in \{\pm 1\}$ is the local root number of $J/L_{\mathfrak{v}}$. The strategy to prove Theorem 1.1 is to similarly decompose the parity of the 2-infinity Selmer rank of J over L into local terms, and compare these place by place. Specifically, results of [41] combined with work of Poonen–Stoll [51] give a decomposition of the parity of $\mathrm{rk}_2(J/L)$ into local terms as detailed below, generalising a theorem of Kramer [26, Theorem 1] for elliptic curves. Before stating this decomposition, we need to introduce some notation.

Notation 1.5. For each place v of K which does not split in L, define the *local norm map*

$$N_{L_{\mathfrak{v}}/K_v} : J(L_{\mathfrak{v}}) \to J(K_v)$$

sending $P \in J(L_{\mathfrak{v}})$ to

$$N_{L_{\mathfrak{v}}/K_v}(P) = \sum_{\sigma \in \mathrm{Gal}(L_{\mathfrak{v}}/K_v)} \sigma(P).$$

Note that, as a quotient of $J(K_v)/2J(K_v)$, the cokernel of this map is a finite-dimensional $\mathbb{F}_2$-vector space.

Define also the invariant $\epsilon(C/K_v) \in \{0, 1\}$ by setting

$$\epsilon(C/K_v) = \begin{cases} 1 & C/K_v \text{ is deficient,} \\ 0 & \text{otherwise.} \end{cases}$$

Here, following [51, Section 8], we say that C/K_v is deficient if C has no K_v-rational divisor of degree $g - 1$.

The relevance of the invariant $\epsilon(C/K_v)$ comes from a result of Poonen and Stoll [51, Theorem 8] characterising the failure of the Shafarevich–Tate group of J/K to have square order (if finite) in terms of the $\epsilon(C/K_v)$. Denoting by C^L/K the quadratic twist of C by L, we define $\epsilon(C^L/K_v)$ similarly. We then have the following decomposition of the parity of $\mathrm{rk}_2(J/L)$ into local terms.

Theorem 1.6 (=Theorem 2.1). *We have*

$$(-1)^{rk_2(J/L)} = \prod_{\substack{v \text{ place of } K \\ v \text{ non-split in } L}} (-1)^{\epsilon(C/K_v)+\epsilon(C^L/K_v)+\dim J(K_v)/N_{L_{\mathfrak{v}}/K_v} J(L_{\mathfrak{v}})}.$$

Ideally, one might hope that the local terms contributing to $w(J/L)$ and $(-1)^{\mathrm{rk}_2(J/L)}$ simply agree place by place. However, this turns out not to be the case, and so, the strategy hinges on identifying the discrepancy between these local terms as a quantity which vanishes globally. To

this end, we conjecture the following, generalising a formula of Kramer–Tunnell [27] for elliptic curves.

Conjecture 1.7. *Let K be a local field of characteristic different from 2. Let L/K be a quadratic extension, let C/K be a hyperelliptic curve and denote by J/K the Jacobian of C. Then we have*

$$w(J/L) = (\Delta_C, L/K)(-1)^{\varepsilon(C/K)+\varepsilon(C^L/K)+\dim J(K)/N_{L/K}J(L)}.$$

Here, the quantity Δ_C is the discriminant of $f(x)$ for any Weierstrass equation $y^2 = f(x)$ defining C, and $(\Delta_C, L/K) \in \{\pm 1\}$ is the Hilbert/Artin symbol of Δ_C with respect to the extension L/K.[†]

Returning now to the case where L/K is a quadratic extension of number fields and C is a hyperelliptic curve defined over K, by the product formula for Hilbert symbols, we have

$$\prod_{\substack{v \text{ place of } K \\ v \text{ non-split in } L}} (\Delta_C, L_{\mathfrak{v}}/K_v) = 1.$$

In particular, we see from (1.4) and Theorem 1.6 that Conjecture 1.7 implies the 2-parity conjecture for J/L. We will prove Conjecture 1.7 under the assumptions on the reduction of C appearing in the statement of Theorem 1.1, hence proving that result. Specifically, our second main result is the following.

Theorem 1.8. *Conjecture 1.7 holds in the following cases:*

- $K = \mathbb{R}$,
- K *has odd residue characteristic, and either L/K is unramified or J/K has semistable reduction,*
- K *is a finite extension of $\mathbb{Q}_2$, L/K is unramified and either J/K has good reduction or $g = 2$ and J/K has semistable reduction,*
- K *is a finite extension of $\mathbb{Q}_2$, J/K has good ordinary reduction, and $K(J[2])/K$ has odd degree.*

Remark 1.9. More generally, Conjecture 1.7 holds if there is an odd degree Galois extension F/K over which C satisfies the conditions of Theorem 1.8 with L/K replaced by FL/F; see Section 4.

As further evidence for Conjecture 1.7, we show that the cases above (and, in fact, substantially fewer) are sufficient to deduce Conjecture 1.7 from the 2-parity conjecture via a global-to-local argument, at least for curves arising via base change from a number field.

Theorem 1.10 (=Theorem 8.1). *Let K be a number field, C/K a hyperelliptic curve, J/K its Jacobian and v_0 a place of K. If the 2-parity conjecture holds for J over every quadratic extension of K, then Conjecture 1.7 holds for J/K_{v_0} and every quadratic extension L/K_{v_0}.*

Remark 1.11. We remark that Conjecture 1.7 makes sense (and, surprisingly, is not entirely vacuous) in genus 0. Indeed, for a quadratic extension L/K of local fields of characteristic different from 2, consider a hyperelliptic curve $C : y^2 = f(x)$ where $f(x) \in K[x]$ is a squarefree polyno-

---

[†] Given another Weierstrass equation $y^2 = h(x)$ for C, the discriminants of $f(x)$ and $h(x)$ differ by a square in K, and hence the term $(\Delta_C, L/K)$ is independent of the choice of Weierstrass equation.

mial of degree 1 or 2. The Jacobian of C is trivial, so the root number and cokernel of the local norm map are trivial also. Further, C/K (resp. C^L/K) is deficient if and only if it has no K-point. It is then easy to check that $(\Delta_C, L/K) = (-1)^{\epsilon(C/K) + \epsilon(C^L/K)}$ for any quadratic extension L/K.

1.4 | Comparison with work of Kramer–Tunnell

Conjecture 1.7 has its origins in work of Kramer–Tunnell. Specifically, for a local field K, a separable quadratic extension L/K and an elliptic curve E/K, Kramer–Tunnell [27] conjectured the formula

$$w(E/K)w(E^L/K) = (-\Delta_E, L/K)(-1)^{\dim E(K)/N_{L/K}E(L)}, \qquad (1.12)$$

and proved it in many cases, including in every instance when K has odd residue characteristic. This conjecture is now known in all cases thanks to subsequent work of Dokchitser–Dokchitser [17] and Česnavičius–Imai [10].

By [8, Proposition 3.11], we have

$$w(E/L) = w(E/K)w(E^L/K)(-1, L/K),$$

whilst $\epsilon(E/K) = 0$ for every local field K and elliptic curve E/K. Thus, Conjecture 1.7 specialises to Equation 1.12 when C/K is an elliptic curve.

The presence of the new terms $\epsilon(C/K)$ and $\epsilon(C^L/K)$ in the purely local Conjecture 1.7, which are 'forced' by global considerations concerning the possible failure of the Shafarevich–Tate group of a principally polarised abelian variety to have square order (see Section 2), is a key new feature of this work. These terms also place constraints on possible proofs of Conjecture 1.7. Indeed, $\epsilon(C/K)$ is not a function purely of the Jacobian of C (as in Remark 1.11, $\epsilon(C/K)$ can be non-trivial even for curves of genus 0!). A lot of the technical difficulty in this work is involved in relating invariants defined in terms of the Jacobian of C, such as the cokernel of the local norm map, to the invariants $\epsilon(C/K)$, $\epsilon(C^L/K)$ and $(\Delta_C, L/K)$, which have no obvious meaning for general abelian varieties.

As above, the Kramer–Tunnell formula (1.12) is known to hold for local fields of characteristic 2 and separable quadratic extensions L/K. It is thus tempting to extend the scope of Conjecture 1.7 to include such extensions (especially in light of the work of Česnavičius–Imai [10] who reduce (1.12) over local fields of characteristic 2 to the corresponding conjecture for finite extensions of $\mathbb{Q}_2$). However, since we prove no instances of Conjecture 1.7 over local fields of characteristic 2 in this work, we have elected not to do this.

1.5 | Overview of the paper

In Section 2, we explain how to deduce Theorem 1.6 by combining results of [41] with work of Poonen–Stoll [51].

In Section 3, we recall and prove some basic properties of the local norm map for general abelian varieties. Of particular use later is Lemma 3.4 which, for non-archimedean local fields of odd residue characteristic, expresses the order of the cokernel of the local norm map in terms of Tamagawa numbers, generalising a result of Kramer–Tunnell [27, Corollary 7.6] for elliptic curves.

In Section 4, we prove some compatibility results concerning the behaviour of Conjecture 1.7 under quadratic twist, and under odd-degree Galois extension of the base field.

Across Sections 5, 6, we collect and prove some basic results concerning, respectively, 2-torsion in Jacobians of hyperelliptic curves, and criteria for determining when a hyperelliptic curve over a local field K is deficient. Whilst much of this material is standard, Proposition 6.7, which characterises deficiency for a particular class of hyperelliptic curves (essentially those with a K-rational theta characteristic), may be of independent interest.

In Section 7, we combine the results of Sections 5, 6 to deduce some simple cases of Conjecture 1.7. Namely, we establish Conjecture 1.7 when K is archimedean, and when K has odd residue characteristic and J/K has good reduction. Then, in Section 8, we show that these special cases are already enough to deduce Theorem 1.10.

With the exception of the short Sections 16 and 17 (which, respectively, consider Conjecture 1.7 for finite extensions of $\mathbb{Q}_2$, and tie together results from previous sections to prove 1.1, 1.8), the remainder of the paper splits into two parts. Firstly, in Sections 9, 10, we consider Conjecture 1.7 when the extension L/K is unramified, proving it completely in this case when K has odd residue characteristic. We do this by analysing the minimal proper regular model of C. The key fact making Conjecture 1.7 accessible here is that the formation of the minimal regular model commutes with unramified base change; this enables a comparison between invariants of C and those of its unramified quadratic twist. The central technical result of these sections is Theorem 10.2, which we formulate for general curves, and which shows that the quantity

$$2^{\epsilon(C/K)} \frac{|\Phi(\bar{k})|}{|\Phi(k)|},$$

viewed as an element of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, behaves well under quite general twisting. Here, k is the residue field of K and Φ is the Néron component group of the Jacobian of C. We would also like to advertise Proposition 10.8, which is a by-product of the proof of Theorem 10.2, and which gives a relatively simple way of computing the Tamagawa number of the Jacobian of an arbitrary curve, modulo rational squares, as a function of its minimal regular model. This result plays a prominent role in simplifying computations in Section 14.

Finally, across Sections 11–15, we prove Conjecture 1.7 when C/K has semistable reduction and when L/K is a ramified quadratic extension of local fields with odd residue characteristic. Roughly speaking, once again, our strategy is to encode each of the invariants appearing in Conjecture 1.7 in terms of the minimal proper regular models of both C and C^L. However, since now L/K is ramified, the minimal regular model of C^L can be significantly different to that of C, making it hard to relate the relevant invariants. We overcome this by fixing a Weierstrass equation $y^2 = f(x)$ for C and drawing on the explicit description of the minimal regular models of C and C^L in terms of clusters (certain combinatorial objects encoding the distances between the roots of $f(x)$) afforded by the works [18] and [20]. This essentially reduces Conjecture 1.7 to a purely combinatorial question about clusters, though one that still seems far from straightforward. We split the resulting analysis into two parts. Firstly, in Proposition 13.20, we give an explicit description in terms of clusters of the group $\mathfrak{B}_{C/K}$ introduced by Betts–Dokchitser in [4]; this group packages together information about the Tamagawa number of the Jacobian of C over both K and L, but seems simpler to describe than each of these quantities. Then, in Section 14, we study the minimal regular model of C^L, describing in terms of clusters the Tamagawa number of the Jacobian of C^L modulo rational squares; see Corollary 14.31. Finally, in Section 15, we combine these results to establish the sought case of Conjecture 1.7.

Notation and conventions

For a field K, we denote by $\bar{K}$ a (fixed once and for all) algebraic closure of K, and denote by $K^s \subseteq \bar{K}$ the separable closure of K. We denote by $G_K = \mathrm{Gal}(K^s/K)$ the absolute Galois group of K.

1.5.1 | Hyperelliptic curves

By a hyperelliptic curve C over a field K, we mean a smooth, proper, geometrically connected curve of genus $g \geqslant 2$, defined over K, and admitting a finite separable morphism $C \to \mathbb{P}^1_K$ of degree 2. When K has characteristic different from 2, one can always find a separable polynomial $f(x) \in K[x]$ of degree $2g + 1$ or $2g + 2$ such that C is isomorphic to the curve given by gluing the affine schemes

$$U_1 = \mathrm{Spec}\,\frac{K[x, y]}{y^2 - f(x)} \quad \text{and} \quad U_2 = \mathrm{Spec}\,\frac{K[u, v]}{v^2 - u^{2g+2}f(1/u)},$$

via the relations $x = 1/u$ and $y = x^{g+1}v$. By an abuse of notation, we say that C is given by the Weierstrass equation $y^2 = f(x)$, and refer to elements of $U_2(\bar{K}) \setminus U_1(\bar{K})$ as the points at infinity. There are two such points if $\deg(f)$ is even, and 1 if $\deg(f)$ is odd. We denote by ι the hyperelliptic involution of C. For $C : y^2 = f(x)$, this is the automorphism $(x, y) \mapsto (x, -y)$.

When $\mathrm{char}(K) \neq 2$, we define the discriminant $\Delta_C \in K^\times$ of a hyperelliptic curve given by a Weierstrass equation $C : y^2 = f(x)$ by the formula given in [32, Seciton 2]. One sees from that work that, up to squares in $K^\times$, this both agrees with the polynomial discriminant of $f(x)$ and is independent of the choice of Weierstrass equation for C/K. In particular, we will often consider $\Delta_C \in K^\times/K^{\times 2}$ without reference to a Weierstrass equation for C. Further, if we write $f(x) = c_f f_0(x)$ where c_f is the leading coefficient of $f(x)$ and $f_0(x)$ is monic, then the discriminants of $f(x)$ and $f_0(x)$ differ by $c_f^{2\deg(f)-2}$, and hence agree modulo squares in K. In particular, the class $\Delta_C \in K^\times/K^{\times 2}$ does not feel the leading coefficient of $f(x)$.

1.5.2 | Quadratic twists

Let K be a field of characteristic different from 2, and L/K a quadratic extension. For a hyperelliptic curve C/K, we denote by C^L/K the quadratic twist of C by L/K. This is the twist of C/K corresponding to the 1-cocycle

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \{1, \iota\} \leqslant \mathrm{Aut}_L(C).$$

Suppose that C/K is given by a Weierstrass equation $y^2 = f(x)$, and that $L = K(\sqrt{d})$ for some $d \in K^\times$. Then C^L/K is given by the Weierstrass equation $y^2 = df(x)$. In particular, it follows from the discussion on hyperelliptic discriminants above that, as elements of $K^\times/K^{\times 2}$, we have $\Delta_C = \Delta_{C^L}$.

For an abelian variety A/K, we similarly denote by A^L/K the quadratic twist of A by L/K, which corresponds to the 1-cocycle

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \{\pm 1\} \leqslant \mathrm{Aut}_L(A).$$

Denote by $\chi : G_K \to \{\pm 1\}$ the quadratic character corresponding to L/K. Then, there is a K^s-isomorphism $\psi : A \xrightarrow{\sim} A^L$ such that, for all $\sigma \in G_K$, the composition $\psi^{-1} \circ {}^\sigma\psi$ is multiplication by $\chi(\sigma)$ on A, where ${}^\sigma\psi$ denotes the unique isomorphism $A \to A^L$ acting as $\sigma \circ \psi \circ \sigma^{-1}$ on K^s-points. In particular, ψ restricts to an isomorphism of G_K-modules $A[2] \cong A^L[2]$.

Since the hyperelliptic involution on C induces multiplication by -1 on its Jacobian J/K, the Jacobian of C^L/K coincides with J^L/K.

1.5.3 | Galois cohomology

For a profinite group G, a discrete G-module M and integer $i \geqslant 0$, we denote by $H^i(G, M)$ the ith cohomology group of G with coefficients in M, as defined in, for example, [24]. We denote by M^G the subgroup of elements of M fixed by G. For $g \in G$, we denote by M^g the subgroup of elements fixed by g.

When $G = G_K$ for a field K, we will often write $H^i(K, M)$ in place of $H^i(G_K, M)$. Similarly, for a Galois extension L/K and a discrete $\mathrm{Gal}(L/K)$-module M, we often write $H^i(L/K, M)$ in place of $H^i(\mathrm{Gal}(L/K), M)$.

1.5.4 | Notation for number fields and local fields

For a number field K, we denote by $\mathcal{O}_K$ the ring of integers of K. For a place v of K, K_v will denote the corresponding completion.

By a local field K, we mean a locally compact valued field. Thus, K is isomorphic (as a valued field) to one of $\mathbb{R}$, $\mathbb{C}$, or a finite extension of either $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$ for a prime p. For a non-archimedean local field K, we take the following notation:

$\mathcal{O}_K$	ring of integers of K,
k	residue field of K,
π	a choice of uniformiser of K,
$v : \bar{K}^\times \to \mathbb{Q}$	valuation on $\bar{K}$ normalised with respect to K, so that $v(\pi) = 1$,
$\mathfrak{m}$	maximal ideal of the ring of integers of $\bar{K}$,
K^{nr}	maximal unramified extension of K,
$(a, L/K)$	Artin symbol of $a \in K^\times$ in a Galois extension L/K. We will usually take L/K quadratic, in which case we regard this symbol as being valued in $\{\pm 1\}$.

1.5.5 | Notation for curves and abelian varieties

For a smooth, proper, geometrically connected curve X over a local field K, we define $\epsilon(X/K) \in \{0, 1\}$ to be equal to 1 if X is deficient over K, and equal to 0 else. Thus, $\epsilon(X/K) = 1$ if and only if X has a K-rational divisor of degree $g - 1$, where g is the genus of X.

Throughout the paper, for a field K, C/K will almost always denote a hyperelliptic curve over K, g will denote the genus of C and J/K will denote the Jacobian of C.

For an abelian variety A over a field K (usually the Jacobian of a hyperelliptic curve C), we take the following notation.

For K a number field:

$\text{rk}_2(A/K)$ the 2-infinity Selmer rank of A/K,

$\text{Sel}^2(A/K)$ the 2-Selmer group of A/K,

Ш(A/K) the Shafarevich–Tate group of A/K,

Ш$_{\text{nd}}(A/K)$ the quotient of Ш(A/K) by its maximal divisible subgroup,

$w(A/K)$ the global root number of A/K.

For K a non-archimedean local field:

Φ the component group of the special fibre of the Néron model of A/K;
  we often refer to this as the Néron component group of A,

$c(A/K)$ the Tamagawa number of A/K. By definition, this is the order of the group $\Phi(k)$
   of k-rational points of Φ,

$w(A/K)$ the local root number of A/K,

$N_{L/K}$ for L/K separable quadratic, denotes the norm map $A(L) \to A(K)$
   sending $P \in A(L)$ to $N_{L/K}(P) := \sum_{\sigma \in \text{Gal}(L/K)} \sigma(P)$.

2 | 2-SELMER GROUPS IN QUADRATIC EXTENSIONS

In this section, we combine results of [41] and [51] to deduce Theorem 1.6. Let L/K be a quadratic extension of number fields, let C/K be a hyperelliptic curve and let J/K denote the Jacobian of C. Further, denote by $\text{rk}_2(J/K)$ the 2-infinity Selmer rank of J/K, and recall from Notation 1.5 the definitions of the local norm map and the invariant $\epsilon(C/K_v)$ for a place v of K. Let C^L/K (resp. J^L/K) denote the quadratic twist of C (resp. J) by L/K.

Theorem 2.1 (=Theorem 1.6). *We have*

$$rk_2(J/L) \equiv \sum_{\substack{v \text{ place of } K \\ v \text{ non-split in } L/K}} \left(\epsilon(C/K_v) + \epsilon(C^L/K_v) + \dim J(K_v)/N_{L_{\mathfrak{v}}/K_v} J(L_{\mathfrak{v}}) \right) \quad (\bmod 2).$$

Proof. By [41, Theorem 10.12], we have

$$\dim \text{Sel}^2(J/K) + \dim \text{Sel}^2(J^L/K) \equiv \sum_{\substack{v \text{ place of } K \\ v \text{ non-split in } L/K}} \dim J(K_v)/N_{L_{\mathfrak{v}}/K_v} J(L_{\mathfrak{v}}) \ (\bmod 2),$$

where here $\text{Sel}^2(J/K)$ denotes the 2-Selmer group of J/K (and similarly for J^L/K). Consequently (cf. [41, proof of Theorem 10.20]), we have

$$\text{rk}_2(J/L) \equiv \dim \text{Ш}_{\text{nd}}(J/K)[2] + \dim \text{Ш}_{\text{nd}}(J^L/K)[2]$$

$$+ \sum_{\substack{v \text{ place of } K \\ v \text{ non-split in } L}} \dim J(K_v)/N_{L_{\mathfrak{v}}/K_v} J(L_{\mathfrak{v}}), \quad (\bmod 2),$$

where $\mathrm{III}_{\mathrm{nd}}(J/K)$ denotes the quotient of the Shafarevich–Tate group of J/K by its maximal divisible subgroup. It follows from [51, Theorem 11] that

$$\dim \mathrm{III}_{\mathrm{nd}}(J/K)[2] \equiv \sum_{v \text{ place of } K} \epsilon(C/K_v) \qquad \text{and}$$

$$\dim \mathrm{III}_{\mathrm{nd}}(J^L/K)[2] \equiv \sum_{v \text{ place of } K} \epsilon(C^L/K_v),$$

where both congruences are modulo 2. For the second equality, we are using that the Jacobian of C^L coincides with the quadratic twist J^L. Since C and C^L are isomorphic over K_v for each place v that splits in L/K, the result follows. $\qquad\square$

Remark 2.2. One of the key reasons for working with Jacobians of hyperelliptic curves in this paper is that the quadratic twist J^L is again the Jacobian of an explicit curve: the quadratic twist C^L. This allows us to give an explicit description of the parity of both $\dim \mathrm{III}_{\mathrm{nd}}(J/K)[2]$ and $\dim \mathrm{III}_{\mathrm{nd}}(J^L/K)[2]$ in terms of deficiency.

3 | BASIC PROPERTIES OF THE LOCAL NORM MAP

In this section, we prove some basic properties of the cokernel of the local norm map. Take K to be a local field of characteristic different from 2, and let L/K be a quadratic extension. We work with arbitrary principally polarised abelian varieties since everything goes through in this setting. Thus, for now we fix a principally polarised abelian variety A/K, and denote by A^L the quadratic twist of A by L/K. Denote by $N_{L/K} : A(L) \to A(K)$ the local norm map, sending $P \in A(L)$ to $\sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(P)$. Further, denote by $\chi : G_K \to \{\pm 1\}$ the quadratic character corresponding to L/K.

Lemma 3.1. *We have*

$$\dim A(K)/2A(K) = \dim A^L(K)/2A^L(K).$$

Proof. Let $\delta : A(K)/2A(K) \hookrightarrow H^1(K, A[2])$ be the connecting map associated to the multiplication-by-2 Kummer sequence for A. By [49, Proposition 4.10], the image of δ is a maximal isotropic subspace of $H^1(K, A[2])$ with respect to the pairing coming from cup-product and the local invariant map. Since $A[2] \cong A^L[2]$ as G_K-modules, this gives

$$\dim A(K)/2A(K) = \frac{1}{2} \dim H^1(K, A[2]) = \dim A^L(K)/2A^L(K),$$

as desired. $\qquad\square$

From the definition of the quadratic twist A^L, we have an L-isomorphism $\psi : A \xrightarrow{\sim} A^L$ such that, for all $\sigma \in G_K$, the composition $\psi^{-1} \circ {}^\sigma\psi$ is multiplication by $\chi(\sigma)$ on A. The map ψ^{-1} identifies $A^L(L)$ with $A(L)$, and identifies $A^L(K)$ with $\ker(N_{L/K} : A(L) \to A(K))$. The local norm map $A^L(L) \to A^L(K)$ then identifies with the map sending $P \in A(L)$ to $P - \sigma(P)$. To avoid confusion, we denote this map by $N_{L/K}^L$.

Lemma 3.2. *The group $A(K)/N_{L/K}A(L)$ is a finite-dimensional $\mathbb{F}_2$-vector space and*

$$\dim A(K)/N_{L/K}A(L) = \dim A^L(K)/N_{L/K}^L A(L).$$

Proof. That $A(K)/N_{L/K}A(L)$ is a finite-dimensional $\mathbb{F}_2$-vector space follows from the fact that $2A(K) \subseteq N_{L/K}A(L)$ along with the well-known finiteness of $A(K)/2A(K)$. Next, consider the map

$$\theta : N_{L/K}A(L)/2A(K) \longrightarrow N_{L/K}^L A(L)/2A^L(K)$$

sending $N_{L/K}(P)$ to $N_{L/K}^L(P)$. This is readily checked to be a (well-defined) isomorphism. The result now follows from Lemma 3.1. $\qquad\square$

Now let $\mathrm{Res}_{L/K}A$ denote the Weil restriction of scalars of A from L to K. This is an abelian variety over K of dimension $2\dim A$ which represents the functor $T \mapsto A(T \times_K L)$. As explained in [38, Section 2] (see also [37, Proposition 4.1]), denoting by γ the involution of $A \times A$ swapping the factors, $\mathrm{Res}_{L/K}A$ can be described as the twist of $A \times A$ corresponding to the 1-cocycle $G_K \to \mathrm{Aut}_{K^s}(A \times A)$ defined by

$$\sigma \mapsto \begin{cases} \mathrm{id} & \chi(\sigma) = 1, \\ \gamma & \chi(\sigma) = -1. \end{cases}$$

This identifies $(\mathrm{Res}_{L/K}A)(K)$ with the L-points of A diagonally embedded in $A(\bar{K}) \times A(\bar{K})$, realising the functor of points description for $T = K$.

As above, both $\mathrm{Res}_{L/K}A$ and $A \times A^L$ are twists of $A \times A$, and one checks that the endomorphism of $A \times A$ given by $(P, Q) \mapsto (P + Q, P - Q)$ descends to an isogeny $\phi : \mathrm{Res}_{L/K}A \to A \times A^L$. On K-points, this is just the map

$$(N_{L/K}, N_{L/K}^L) : (\mathrm{Res}_{L/K}A)(K) = A(L) \longrightarrow A(K) \times A^L(K). \tag{3.3}$$

(See [37, Sections 4 and 5] for generalisations of this isogeny when L/K is replaced by a general finite Galois extension.)

We exploit the isogeny ϕ to prove the final lemma of this section, which expresses the cokernel of the local norm map in terms of Tamagawa numbers. The special case of this for elliptic curves is due to Kramer and Tunnell [27, Corollary 7.6], although the proof is different. Recall from Section 1.5.5 that $c(A/K)$ denotes the Tamagawa number of A/K.

Lemma 3.4. *Assume that the residue characteristic of K is odd. Then*

$$\dim A(K)/N_{L/K}A(L) = \mathrm{ord}_2 \frac{c(A/K)c(A^L/K)}{c(A/L)}.$$

Proof. To ease notation, write $X = \mathrm{Res}_{L/K}A$ and $Y = A \times A^L$. With ϕ as above, since K has odd residue characteristic, it follows from a formula of Schaefer [56, Lemma 3.8] that

$$\mathrm{ord}_2 \frac{|Y(K)/\phi X(K)|}{|X(K)[\phi]|} = \mathrm{ord}_2 \frac{c(Y/K)}{c(X/K)} = \mathrm{ord}_2 \frac{c(A/K)c(A^L/K)}{c(A/L)}, \tag{3.5}$$

the last equality following from [33, Proposition 3.19] (see also [38, Proof of Proposition 2]). From the description (3.3) of the map ϕ on K-points, one sees that $X(K)[\phi] \cong A(K)[2]$ and that we have a short exact sequence

$$0 \longrightarrow A^L(K)/2A^L(K) \longrightarrow Y(K)/\phi X(K) \longrightarrow A(K)/N_{L/K}A(L) \longrightarrow 0, \qquad (3.6)$$

the first map induced by inclusion into the second factor, and the second map being the projection onto the first factor. Since K has odd residue characteristic, we have (cf. [56, Proposition 3.9], e.g.)

$$\dim A^L(K)/2A^L(K) = \dim A^L(K)[2] \quad (= \dim A(K)[2]).$$

The result now follows by combining this last observation with (3.5) and (3.6). $\qquad\square$

4 | COMPATIBILITY RESULTS

In this section, we prove several compatibility results for Conjecture 1.7. These provide some evidence in favour of the conjecture and will also be used to make some reductions as part of the proof of Theorem 1.8.

In what follows, K denotes a local field of characteristic different from 2. Let L/K be a quadratic extension and let C/K be a hyperelliptic curve.

4.1 | Odd degree Galois extensions

Lemma 4.1. *Every individual term in Conjecture 1.7 is unchanged under odd degree Galois extension of the base field. In particular, if F/K is an odd degree Galois extension, then Conjecture 1.7 holds for C/K and the extension L/K if and only if it holds for C/F and the extension LF/F.*

Proof. That the term $(\Delta_C, L/K)$ is invariant under odd degree extensions (not necessarily Galois) is standard. Similarly, it is not hard to show that the terms involving deficiency of C and its twist are also individually invariant under arbitrary odd degree extensions (cf. Lemma 6.4 for a more general result which implies this). The statement for each of the root numbers is also standard; see, for example, [15, Lemma A.1 and Proposition A.2] or [27, Proposition 3.4]. For the cokernel of the local norm map, the statement for elliptic curves is [27, Proposition 3.5] and the argument for general abelian varieties is identical. $\qquad\square$

4.2 | First compatibility with quadratic twist

Lemma 4.2. *Conjecture 1.7 holds for C/K and the extension L/K if and only if it holds for C^L/K and the same extension.*

Proof. Since the root number and terms involving deficiency appear symmetrically between J and J^L in Conjecture 1.7, it suffices to show that

$$(\Delta_C, L/K) = (\Delta_{C^L}, L/K)$$

and

$$\dim J(K)/N_{L/K}J(L) \equiv \dim J^L(K)/N^L_{L/K}J(L) \text{ (mod 2)}.$$

For the first equality, one checks readily that Δ_C and Δ_{C^L} lie in the same class in $K^\times/K^{\times 2}$ (cf. Section 1.5.2). The second statement follows from Lemma 3.2. ∎

4.3 | Second compatibility with quadratic twist

The second compatibility result involving quadratic twist is more subtle. That such a compatibility result should exist for elliptic curves was discussed in the original paper of Kramer and Tunnell [27, remark following Proposition 3.3] and the result was later proven (again for elliptic curves) by Klagsbrun, Mazur and Rubin [25, Lemma 5.6]. The key step in that proof is to establish the following congruence. In order to state it, fix distinct quadratic extensions L_1/K and L_2/K, and denote by L_3/K the third quadratic subextension of L_1L_2/K.

Lemma 4.3. *Let A/K be a principally polarised abelian variety. Then we have*

$$\dim A(K)/N_{L_1/K}A(L_1) + \dim A(K)/N_{L_2/K}A(L_2) \equiv \dim A^{L_1}(K)/N_{L_3/K}A^{L_1}(L_3) \text{ (mod 2)}.$$

Proof. The case where A/K is an elliptic curve is [25, Lemma 5.6] and the argument is essentially the same. Let $L_0 = K$ and for each $i = 1, 2, 3$ identify $A^{L_i}[2]$ with $A[2]$ as G_K-modules in the usual way. For each i, let X_i denote the image of $A^{L_i}(K)/2A^{L_i}(K)$ under the map

$$A^{L_i}(K)/2A^{L_i}(K) \xrightarrow{\delta^{L_i}} H^1(K, A^{L_i}[2]) = H^1(K, A[2]),$$

where δ^{L_i} is the connecting homomorphism associated to the multiplication-by-2 Kummer sequence for A^{L_i}. By [36, Proposition 5.2], for $i = 1, 2, 3$, we have

$$A(K)/N_{L_i/K}A(L_i) \cong X_0/(X_0 \cap X_i).$$

Similarly, we have

$$A^{L_1}(K)/N_{L_3/K}A^{L_1}(L_3) \cong X_1/(X_1 \cap X_2).$$

In the elliptic curve case treated in [25], it is shown that each X_i is a maximal isotropic subspace with respect to a certain quadratic form on $H^1(K, A[2])$. The result is then deduced from [25, Corollary 2.5] which is a general result concerning the parity of the dimension of intersections of maximal isotropic subspaces. For general principally polarised abelian varieties, the fact that each X_i is a maximal isotropic subspace for the natural generalisation of this quadratic form is detailed in [41, Section 10.1]. The one difference from the case of elliptic curves is that now the quadratic form (in general) takes values in $\mathbb{Z}/4\mathbb{Z}$, rather than just $\mathbb{Z}/2\mathbb{Z}$ as is assumed in [25, Corollary 2.5]. However, one readily verifies that this assumption is not used in the proof of [25, Corollary 2.5]. ∎

We now return to the case where C/K is a hyperelliptic curve and J/K is its Jacobian.

Corollary 4.4. *Conjecture 1.7 for J/K and the extensions L_1/K and L_2/K implies Conjecture 1.7 for J^{L_1}/K and the extension L_3/K.*

Proof. By [8, Proposition 3.11], for any quadratic extension L/K, we have

$$w(J/L) = ((-1)^g, L/K)w(J/K)w(J^L/K), \tag{4.5}$$

where g is the genus of C (the cited result is only stated for elliptic curves, but the proof generalises verbatim to give the claimed formula). From (4.5), it follows that

$$w(J/L_1)w(J/L_2) = w(J^{L_1}/L_3).$$

Further, by standard properties of Hilbert symbols and the fact that the discriminants of C and any quadratic twist of C differ by squares, we have

$$(\Delta_C, L_1/K)(\Delta_C, L_2/K) = (\Delta_{C^{L_1}}, L_3/K).$$

Since we also have

$$\epsilon(C/K) + \epsilon(C^{L_1}/K) + \epsilon(C/K) + \epsilon(C^{L_2}/K) \equiv \epsilon(C^{L_1}/K) + \epsilon(C^{L_2}/K) \pmod 2$$

$$= \epsilon(C^{L_1}/K) + \epsilon((C^{L_1})^{L_3}/K),$$

the result follows from Lemma 4.3. $\qquad\square$

Remark 4.6. For a local field K and hyperelliptic curve C/K, it follows from Lemma 4.2 and Corollary 4.4 that, in order to prove Conjecture 1.7 for C/K and all quadratic extensions of K, it suffices to prove the same result but with C replaced by an arbitrary quadratic twist.

5 | TWO TORSION IN THE JACOBIAN OF A HYPERELLIPTIC CURVE

For this section, let K be a field of characteristic different from 2. Let $C/K : y^2 = f(x)$ be a hyperelliptic curve of genus g and let J/K be its Jacobian. Denote by $\mathcal{W}$ the G_K-set of ramification points of the x-coordinate morphism $C \to \mathbb{P}^1$. Thus, $\mathcal{W}$ consists of the points $(r, 0)$ for r a root of $f(x)$, along with the unique point at infinity on C if $\deg(f)$ is odd. As G_K-modules, we then have

$$J[2] \cong \ker\left(\mathbb{F}_2^{\mathcal{W}} \xrightarrow{\Sigma} \mathbb{F}_2\right)/\mathbb{F}_2 D. \tag{5.1}$$

Here, $\mathbb{F}_2^{\mathcal{W}}$ denotes the permutation representation over $\mathbb{F}_2$ on the elements of $\mathcal{W}$, $\Sigma : \mathbb{F}_2^{\mathcal{W}} \to \mathbb{F}_2$ denotes the sum-of-coefficients map, and $D = \sum_{w \in \mathcal{W}} w$. See [50, Section 6] for more details. Noting that $g \geqslant 2$, hence $|\mathcal{W}| > 4$, we see from the above description that $K(J[2])/K$ is the splitting field of $f(x)$.

We now compute the dimension of the rational 2-torsion $J(K)[2]$. The case where $K(J[2])/K$ is cyclic is treated in [12, Theorem 1.4] (but note the erratum [13]) whilst the case where $f(x)$ has an odd degree factor over K is [50, Lemma 12.9]. We will require a slightly more general statement.

In what follows we write $f(x) = c_f f_0(x)$, where $c_f \in K^\times$ is the leading coefficient of $f(x)$, and $f_0(x) \in K[x]$ is monic. To clean up the statement, we also make the following convention.

Convention 5.2. In what follows, if $\deg(f)$ is odd, the rational point at infinity on C is to be interpreted as an odd degree irreducible factor of $f(x)$ over K.

Lemma 5.3. *Let n be the number of irreducible factors of $f(x)$ over K (see Convention 5.2 above). If $f(x)$ has an odd degree factor over K, then*

$$\dim J(K)[2] = n - 2.$$

Otherwise, if each irreducible factor of $f(x)$ has even degree, let F/K be the splitting field of $f(x)$ and let m be the number of quadratic subextensions of F/K over which $f_0(x)$ factors as a product of 2 distinct conjugate polynomials. Then

$$\dim J(K)[2] = \begin{cases} n-1 & g \text{ even,} \\ n-1+ord_2(1+m) & g \text{ odd.} \end{cases}$$

Proof. Denote by G the Galois group of F/K and let M be the G-module $M = \ker(\mathbb{F}_2^{\mathcal{W}} \xrightarrow{\Sigma} \mathbb{F}_2)$. Then, by (5.1), we have an exact sequence

$$0 \longrightarrow \mathbb{F}_2 D \longrightarrow M^G \longrightarrow J[2]^G \longrightarrow \ker\left(H^1(G, \mathbb{F}_2 D) \to H^1(G, M)\right) \longrightarrow 0. \tag{5.4}$$

Now

$$\dim M^G = \ker\left((\mathbb{F}_2^{\mathcal{W}})^G \xrightarrow{\Sigma} \mathbb{F}_2\right) = \begin{cases} n-1 & f(x) \text{ has an odd degree factor over } K, \\ n & \text{else.} \end{cases}$$

Consequently, we must show that $\ker(H^1(G, \mathbb{F}_2 D) \to H^1(G, M))$ has dimension 0 or $ord_2(1+m)$ according, respectively, to whether g is even or odd (note that if $f(x)$ has an odd degree factor over K then $m = 0$).

Now $H^1(G, \mathbb{F}_2 D) = \text{Hom}(G, \mathbb{F}_2 D)$, and the non-trivial homomorphisms from G into $\mathbb{F}_2 D$ correspond to the quadratic subextensions of F/K. Let ϕ be such a homomorphism, corresponding to a quadratic subextension E/K. Then ϕ maps to 0 in $H^1(G, M)$ if and only if there is $\eta \in M$ with $\sigma(\eta) + \eta = \phi(\sigma)D$ for each $\sigma \in G$. Now an element $\eta \in \mathbb{F}_2^{\mathcal{W}}$ satisfying this equation corresponds to a factor of $f_0(x)$ over E, $h(x)$ say, for which $f_0(x) = h(x) \cdot \tau h(x)$, where τ denotes the generator of $\text{Gal}(E/K)$. Since $\frac{1}{2}|\mathcal{W}| = g + 1$, such an η is in the sum-zero part of $\mathbb{F}_2^{\mathcal{W}}$ if and only if g is odd. We conclude from this that the number of non-identity elements in $\ker(H^1(G, \mathbb{F}_2 D) \to H^1(G, M))$ is equal to 0 if g is even, and m if g is odd. This gives the result. $\square$

Now let Δ_f be the discriminant of $f(x)$. It is a square in K if and only if the Galois group of $f(x)$ is a subgroup of the alternating group A_n where $n = \deg f$. As a corollary of Lemma 5.3, we

observe that if $K(J[2])/K$ is cyclic, then whether or not the discriminant of $f(x)$ is a square in K can essentially be detected from the rational 2-torsion in J. In the statement, we continue to impose Convention 5.2.

Corollary 5.5. *Suppose that $K(J[2])/K$ is cyclic. Then Δ_f is a square in K if and only if one of the following holds:*

(i) $(-1)^{\dim J(K)[2]} = 1$ *and either g is odd or $f(x)$ has an odd degree factor over K,*
(ii) $(-1)^{\dim J(K)[2]} = -1$, g *is even, and all factors of $f(x)$ over K have even degree.*

Proof. Let σ be a generator of $\mathrm{Gal}(K(J[2])/K)$. Then Δ_f is a square in K if and only if $\epsilon(\sigma) = 1$, where $\epsilon(\sigma)$ is the sign of σ as a permutation on the roots of $f(x)$. Suppose that σ has cycle type $(d_1, \ldots, d_n)$, so that the d_i are the degrees of the irreducible factors of $f(x)$ over K. Then we have $\epsilon(\sigma) = (-1)^{\sum_{i=1}^{n}(d_i - 1)} = (-1)^{\deg f - n}$. Now $J[2]^\sigma = J(K)[2]$. Moreover, $K(J[2])/K$ contains at most one quadratic subextension, which yields a factorisation of $f_0(x)$ into two distinct conjugate polynomials if and only if each d_i is even. The result now follows from Lemma 5.3. $\qquad\square$

6 | DEFICIENCY

Let K be a local field. Recall from Section 1.5.5 that a (smooth, proper, geometrically connected) curve X/K of genus g is said to be deficient if X has no K-rational divisor of degree $g - 1$. In this section, we collect some results on deficiency which will be of use later. Firstly, we determine the behaviour of deficiency in field extensions. Next, we give some criteria for determining when a hyperelliptic curve is deficient, which apply in particular when $K(J[2])/K$ is cyclic. Finally, for non-archimedean base fields, we recall a criteria due to Poonen and Stoll which describes deficiency of a general curve in terms of its minimal proper regular model.

The first two results mentioned above are a consequence of the following description of deficiency, which arises as part of the proof of [51, Theorem 11]. Consider the short exact sequences of G_K-modules

$$0 \longrightarrow K^s(X)^\times / K^{s\times} \xrightarrow{\mathrm{div}} \mathrm{Div}(X_{K^s}) \longrightarrow \mathrm{Pic}(X_{K^s}) \longrightarrow 0 \tag{6.1}$$

and

$$0 \longrightarrow K^{s\times} \longrightarrow K^s(X)^\times \longrightarrow K^s(X)^\times / K^{s\times} \longrightarrow 0. \tag{6.2}$$

Here, $K^s(X)$ is the function field of X over the separable closure of K, $\mathrm{Div}(X_{K^s})$ is the group of divisors on the base change of X to K^s, $\mathrm{Pic}(X_{K^s})$ is the Picard group of X_{K^s} and the map div sends a rational function on X_{K^s} to its associated divisor.

As explained in the proof of [51, Theorem 11], combining the associated long exact sequences for Galois cohomology, we obtain an exact sequence

$$0 \longrightarrow \mathrm{Pic}(X) \longrightarrow \mathrm{Pic}(X_{K^s})^{G_K} \longrightarrow \mathrm{Br}(K),$$

where $\mathrm{Br}(K) = H^2(K, K^{s\times})$ denotes the Brauer group of K.

Notation 6.3. We denote by ϕ_K the composition

$$\phi_K : \operatorname{Pic}(X_{K^s})^{G_K} \longrightarrow \operatorname{Br}(K) \xrightarrow{\operatorname{inv}_K} \mathbb{Q}/\mathbb{Z},$$

where the first map is the one constructed above, and the second is the local invariant map.

By a result of Lichtenbaum [28] (see also [51, Section 4]), X has a K-rational divisor class of degree $g - 1$. Fix such a class $\mathcal{L} \in \operatorname{Pic}^{g-1}(X_{K^s})^{G_K}$. In the proof of [51, Theorem 11], Poonen–Stoll show that $(g - 1)\phi_K(\mathcal{L}) \in \{0, 1/2\}$, and that X is deficient over K if and only if $(g - 1)\phi_K(\mathcal{L}) = 1/2$.

6.1 | Deficiency in field extensions

Recall that $\epsilon(X/K) \in \{0, 1\}$ is defined to be equal to 1 if X is deficient over K, and equal to 0 otherwise.

Lemma 6.4. *For any finite extension L/K, we have*

$$\epsilon(X/L) \equiv [L : K]\epsilon(X/K) \ (mod \ 2).$$

Proof. Fix a rational divisor class $\mathcal{L}$ of degree $g - 1$ in $\operatorname{Pic}(X_{K^s})^{G_K}$, so that $(g - 1)\phi_K(\mathcal{L}) \in \mathbb{Q}/\mathbb{Z}$ is equal to $\frac{1}{2}$ (resp. 0) if X is deficient over K (resp. is not deficient over K). Then $\mathcal{L}$ also gives a rational divisor class of degree $g - 1$ in $\operatorname{Pic}(X_{K^s})^{G_L}$, and commutativity of the diagram

$$
\begin{array}{ccc}
\operatorname{Br}(K) & \xrightarrow{\operatorname{inv}_K} & \mathbb{Q}/\mathbb{Z} \\
\downarrow{\scriptstyle \operatorname{res}} & & \downarrow{\scriptstyle [L:K]} \\
\operatorname{Br}(L) & \xrightarrow{\operatorname{inv}_L} & \mathbb{Q}/\mathbb{Z}
\end{array}
\tag{6.5}
$$

(see, e.g. [57, Proposition XIII.3.7]) shows that $(g - 1)\phi_L(\mathcal{L}) = [L : K](g - 1)\phi_K(\mathcal{L})$. $\qquad\square$

6.2 | Deficiency for hyperelliptic curves

Now suppose that the characteristic of K is different from 2. Take C/K to be a hyperelliptic curve of genus g and fix a Weierstrass equation $y^2 = f(x)$ for C. Since C has K-rational divisors of degree 2 (arising as the pull-back of rational points on $\mathbb{P}^1_K$), if g is odd, then C is not deficient. Consequently, we impose the following assumption.

Assumption 6.6. For the rest of this subsection, suppose that g is even.

Again using that C has K-rational divisors of degree 2, we see under this assumption that having a K-rational divisor of degree $g - 1$ is equivalent to having a K-rational divisor of any odd degree, which is, in turn, equivalent to having a rational point over some odd degree extension of K. In particular, if $f(x)$ has an odd degree factor over K, then C is not deficient.

Now write $f(x) = c_f f_0(x)$, where c_f is the leading coefficient of $f(x)$ and $f_0(x)$ is monic. The following proposition gives a convenient criterion for testing deficiency in the special case that $f_0(x)$ factors as a product of two conjugate polynomials over some quadratic extension of K.

Proposition 6.7. *Suppose that $f_0(x)$ factors over a quadratic extension F/K as a product of 2 polynomials conjugate under the action of $\mathrm{Gal}(F/K)$. Then C is deficient if and only if $(c_f, F/K) = -1$.*

Remark 6.8. Proposition 6.7 and the discussion before it gives simple criteria for determining whether or not C is deficient under the condition that the polynomial $f_0(x)$ either has an odd degree factor over K, or factors as a product of two conjugate polynomials over some quadratic extension of K. This condition can be expressed intrinsically as saying that C has a K-rational theta characteristic. Indeed, as in Section 5, let $\mathcal{W}$ denote the G_K-set of ramification points of the x-coordinate morphism $C \to \mathbb{P}_K^1$. Further, let $\mathcal{T}$ denote the quotient of the sum-1 part of the permutation module $\mathbb{F}_2^{\mathcal{W}}$ by the diagonal action of $\mathbb{F}_2$. We see from (5.1) that $\mathcal{T}$ is a torsor under $J[2]$. By [42, Section 4] (recall that g is assumed even), the torsor $\mathcal{T}$ can be identified as a G_K-set with the collection of theta characteristics on C_{K^s}, from which the claim follows readily.

Proof of Proposition 6.7. Over F, write $f_0(x) = f_{0a}(x) f_{0b}(x)$ where $f_{0a}(x)$ and $f_{0b}(x)$ are monic and conjugate under the action of $\mathrm{Gal}(F/K)$. As g is assumed even, both $f_{0a}(x)$ and $f_{0b}(x)$ necessarily have odd degree $g + 1$. For each root r of $f(x)$, write $P_r = (r, 0) \in C(K^s)$. For $\star \in \{a, b\}$, consider the degree $g + 1$ divisor

$$D_\star = \sum_{r \text{ root of } f_{0\star}(x)} P_r \quad \in \mathrm{Div}(C_{K^s}).$$

Denote by $\chi : G_K \to \{\pm 1\}$ the quadratic character corresponding to F/K. Then, for all $\sigma \in G_K$, we have

$$\sigma(D_a) = \begin{cases} D_a & \chi(\sigma) = 1, \\ D_b & \chi(\sigma) = -1. \end{cases}$$

Since $\mathrm{div}(y/f_{0b}(x)) = D_a - D_b$, we see that the class of D_a in $\mathrm{Pic}(C_{K^s})$, which we denote $[D_a]$, is invariant under G_K. Further, we see that under the connecting map $\mathrm{Pic}(C_{K^s})^{G_K} \to H^1(K, K^s(C)^\times/K^{s\times})$ associated to (6.1), the class $[D_a]$ maps to the class of the 1-cocycle ρ defined by

$$\rho(\sigma) = \begin{cases} 1 & \chi(\sigma) = 1, \\ y/f_{0b}(x) & \chi(\sigma) = -1. \end{cases}$$

This lifts via the same formula to a 1-cochain valued in $K^s(C)^\times$. The image of ρ under the connecting map $H^1(K, K^s(C)^\times/K^{s\times}) \to H^2(K, K^{s\times}) = \mathrm{Br}(K)$ associated to (6.2) is thus represented by the class of the 2-cocycle α defined by $\alpha(\sigma, \tau) = \rho(\sigma) \cdot {}^\sigma\rho(\tau) \cdot \rho(\sigma\tau)^{-1}$. A straightforward computation shows that $\alpha(\sigma, \tau) = 1$ unless $\chi(\sigma) = -1 = \chi(\tau)$, in which case it is equal to

$$\frac{y}{f_{0b}(x)} \cdot \frac{y}{f_{0a}(x)} = \frac{y^2}{f_0(x)} = c_f.$$

Under $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$, the class of this 2-cocycle is mapped to 0 if c_f is a norm from $F^\times$, and to $1/2$ otherwise. Thus, $(g+1)\phi_K([D_a]) = 1/2$ if and only if $(c_f, F/K) = -1$. $\qquad\square$

Corollary 6.9. *Suppose that $K(J[2])/K$ is cyclic. If C is deficient over K, then (g is even and) every irreducible factor of $f(x)$ over K has even degree. When this is the case, denote by F/K the unique quadratic subextension of $K(J[2])/K$. Then C is deficient if and only if $(c_f, F/K) = -1$.*

Proof. As noted above, we may assume that each irreducible factor of $f(x)$ over K has even degree, in which case $f(x)$ has degree $2g+2$. The assumption that $K(J[2])/K$ is cyclic now ensures that there is indeed a unique quadratic subextension of $K(J[2])/K$, F/K say, and that $f_0(x)$ factors into two conjugate polynomials over F. The result now follows from Proposition 6.7. $\qquad\square$

Remark 6.10. Suppose that we are in the situation of Corollary 6.9, so that (g is even and) $K(J[2])/K$ is cyclic. Let L/K be a quadratic extension, say $L = K(\sqrt{d})$ for some $d \in K^\times$. Then the quadratic twist of C by L/K has Weierstrass equation $C^L : y^2 = df(x)$. As above, we have $\epsilon(C/K) = 0 = \epsilon(C^L/K)$ unless every irreducible factor of $f(x)$ over K has even degree. In this latter case, with F/K as in the statement of Corollary 6.9, we see from that result that

$$(-1)^{\epsilon(C/K)+\epsilon(C^L/K)} = (c_f, F/K)(dc_f, F/K) = (d, F/K).$$

6.3 | Deficiency in terms of the minimal proper regular model

Now suppose that K is a non-archimedean local field, possibly of characteristic 2, and that X/K is a (not necessarily hyperelliptic) curve of genus g. To conclude the section, we recall a characterisation of deficiency in terms of the minimal proper regular model of X. We will make extensive use of this criterion later.

Let $\mathcal{X}/\mathcal{O}_K$ denote the minimal proper regular model of X, and let $\mathcal{X}_{\bar{k}}$ denote the base change to $\bar{k}$ of its special fibre. Let $\{\Gamma_i\}_{i \in I}$ denote the set of irreducible components of $\mathcal{X}_{\bar{k}}$. For each $i \in I$, let d_i denote the multiplicity of Γ_i in $\mathcal{X}_{\bar{k}}$, and let $\mathrm{orb}_{G_k}(\Gamma_i)$ denote the G_k-orbit of Γ_i.

Lemma 6.11. *The curve X is deficient over K if and only if*

$$\gcd_{i \in I}\{d_i \cdot |\mathrm{orb}_{G_k}(\Gamma_i)|\}$$

does not divide $g-1$.

Proof. This is observed by Poonen–Stoll; see [51], remark following the proof of Lemma 16. $\qquad\square$

Remark 6.12. When X/K is a hyperelliptic curve, we have $\gcd_{i \in I}\{d_i \cdot |\mathrm{orb}_{G_k}(\Gamma_i)|\} \in \{1, 2\}$. This follows from [5, Corollary 1.5] and the fact that all hyperelliptic curves have closed points of degree dividing 2.

7 | FIRST CASES OF CONJECTURE 1.7

In this section, we prove Conjecture 1.7 in two cases: when K is archimedean, and when K has odd residue characteristic and J/K has good reduction. It will turn out that these are the only cases needed to prove Theorem 1.10 (in fact, even the case of archimedean K is not necessary for this).

7.1 | Archimedean local fields

Here, we consider Conjecture 1.7 for archimedean local fields. Clearly, the only case of interest is the extension $\mathbb{C}/\mathbb{R}$. Let $C/\mathbb{R}$ be a hyperelliptic curve of genus g and let $J/\mathbb{R}$ be its Jacobian.

Proposition 7.1. *Conjecture 1.7 holds for $C/\mathbb{R}$ and the extension $\mathbb{C}/\mathbb{R}$.*

Proof. We have $w(J/\mathbb{C}) = (-1)^g$ (see, e.g. [54, Lemma 2.1]). Further, by [41, Lemma 10.9 (ii)], we have $|J(\mathbb{R})/N_{\mathbb{C}/\mathbb{R}}J(\mathbb{C})| = 2^{-g}|J(\mathbb{R})[2]|$. Denote by J_{-1} the quadratic twist of J by $\mathbb{C}/\mathbb{R}$, and and denote by C_{-1} the quadratic twist of C by $\mathbb{C}/\mathbb{R}$ similarly. To verify Conjecture 1.7, we must show that

$$(-1)^{\dim J(\mathbb{R})[2]} = (\Delta_C, \mathbb{C}/\mathbb{R})(-1)^{\epsilon(C/K) + \epsilon(C_{-1}/K)}.$$

Now $\mathbb{R}(J[2])/\mathbb{R}$ is cyclic, and $(\Delta_C, \mathbb{C}/\mathbb{R}) = 1$ if and only if Δ_C is a square in $\mathbb{R}$. Consequently, Corollary 5.5 gives $(-1)^{\dim J(\mathbb{R})[2]} = (\Delta_C, \mathbb{C}/\mathbb{R})$, except when g is even and all irreducible factors of $f(x)$ over $\mathbb{R}$ have even degree. In this latter case, the two expressions differ by a sign. Since by Corollary 6.9 (cf. also Remark 6.10), this is exactly the case where $\epsilon(C/K) + \epsilon(C_{-1}/K) = 1$, we have the result. $\qquad\square$

7.2 | Good reduction in odd residue characteristic

Suppose now that L/K is a quadratic extension of non-archimedean local fields of odd residue characteristic. Let C/K be a hyperelliptic curve and J/K its Jacobian. We denote by v the normalised valuation on K.

Proposition 7.2. *Suppose that J has good reduction over K. Then Conjecture 1.7 holds for C and the extension L/K.*

Proof. Since J has good reduction over K, we have $w(J/L) = 1$, so we are reduced to showing that

$$(-1)^{\dim J(K)/N_{L/K}J(L)} = (\Delta_C, L/K)(-1)^{\epsilon(C/K) + \epsilon(C^L/K)}.$$

Suppose first that L/K is unramified. Then [41, Lemma 10.9 (i)] gives $(-1)^{\dim J(K)/N_{L/K}J(L)} = 1$ (this goes back to a result of Mazur [35, Corollary 4.4]). Moreover, the assumption on the reduction of J implies that $K(J[2])/K$ is unramified. Thus, adjoining a square root of Δ_C to K produces an unramified extension. In particular, $v(\Delta_C)$ is even and $(\Delta_C, L/K) = 1$. Finally, Corollary 6.9 gives $(-1)^{\epsilon(C/K) + \epsilon(C^L/K)} = 1$ also.

Now suppose that L/K is ramified. This time, [41, Lemma 10.9 (i)] gives

$$(-1)^{\dim J(K)/N_{L/K}J(L)} = (-1)^{\dim J(K)[2]}.$$

Moreover, as $v(\Delta_C)$ is even, we have $(\Delta_C, L/K) = 1$ if and only if Δ_C is a square in K. We now conclude by Corollary 5.5 and Corollary 6.9. □

8 | GLOBAL CONJECTURES IMPLY INSTANCES OF CONJECTURE 1.7

We have already proven enough cases of Conjecture 1.7 to prove Theorem 1.10.

Theorem 8.1 (=Theorem 1.10). *Let K be a number field, C/K a hyperelliptic curve, J/K its Jacobian and v_0 a place of K. If the 2-parity conjecture holds for J over every quadratic extension F/K, then Conjecture 1.7 holds for J/K_{v_0} and every quadratic extension L/K_{v_0}.*

Proof. Let L/K_{v_0} be a quadratic extension, and write $L = K_{v_0}(\sqrt{\alpha})$. Let S be a finite set of places of K containing all places where J has bad reduction, all places dividing 2, and all archimedean places. Set $T = S - \{v_0\}$.

Now let F/K be a quadratic extension such that:

- each place $v \in T$ splits in F/K,
- there is exactly one place $\mathfrak{v}_0$ of F extending v_0,
- we have $F_{\mathfrak{v}_0} = L$.

Explicitly, we may take $F = K(\sqrt{\beta})$ where $\beta \in K$ is chosen, by weak approximation, to be sufficiently close to α v_0-adically, and sufficiently close to 1 v-adically for all $v \in T$.

With such an extension F/K chosen, for a place v of K which is non-split in F/K, denote by $\mathfrak{v}$ the unique place of F extending v. Then (cf. Theorem 2.1), the products

$$\prod_{\substack{v \text{ place of } K \\ \text{non-split in } F/K}} w(J/F_{\mathfrak{v}}) \quad \text{and} \quad \prod_{\substack{v \text{ place of } K \\ \text{non-split in } F/K}} (\Delta_C, F_{\mathfrak{v}}/K_v)(-1)^{\dim J(K_v)/N_{F_{\mathfrak{v}}/K_v}J(F_{\mathfrak{v}})+\varepsilon(C/K_v)+\varepsilon(C^F/K_v)}$$

are equal to $w(J/F)$ and $(-1)^{\mathrm{rk}_2(J/F)}$, respectively, and hence, agree under the assumption that the 2-parity conjecture holds for J over F.

On the other hand, by Proposition 7.2 and our assumptions on F/K, the individual contributions to these products at a place v agree, save possibly at $v = v_0$. Thus, the contributions at $v = v_0$ must agree as well. □

9 | UNRAMIFIED EXTENSIONS

Let K be a non-archimedean local field of characteristic different from 2. In this section, we begin the study of Conjecture 1.7 for unramified quadratic extensions. Thus, we fix a hyperelliptic curve

C/K, and denote by L/K the unique unramified quadratic extension of K. As usual, we denote by J/K the Jacobian of C. Across Sections 9 and 10, we will prove the following:

Proposition 9.1. *Conjecture 1.7 for C/K and the extension L/K holds in each of the following cases:*

(i) *the residue characteristic of K is odd,*
(ii) *the residue characteristic of K is 2 and J/K has good reduction,*
(iii) *the residue characteristic of K is 2, C has genus 2 and J/K has semistable reduction.*

To prove this, the key fact we will exploit is that the formation of Néron models and minimal regular models commutes with unramified base change. As L/K is assumed unramified, this makes the quantities appearing in Conjecture 1.7 comparatively easy to describe and relate to one another (in particular, it allows us to readily relate invariants of C to invariants of the quadratic twist of C by L/K). This enables us to reduce Conjecture 1.7 to a statement which depends only on the curve C considered over the maximal unramified extension of K; see Corollary 9.9. We then prove this statement under the conditions of Proposition 9.1.

Denote by k the residue field of K, and denote by k_L the residue field of L. Further, denote by $\mathfrak{f}(J/K)$ the conductor of J, and denote by Φ the component group of the special fibre of the Néron model of J.

Lemma 9.2. *We have*

$$w(J/L) = (-1)^{\mathfrak{f}(J/K)}$$

and

$$\dim J(K)/N_{L/K}J(L) = \dim H^1(k_L/k, \Phi(k_L)).$$

Proof. For the statement about root numbers, see [9, Corollary 4.6]. The statement concerning the norm map follows from Lemma 3.2 and [35, Proposition 4.3]. □

Lemma 9.2 describes two of the terms appearing in Conjecture 1.7. Moreover, as L/K is unramified, we have

$$(\Delta_C, L/K) = (-1)^{v(\Delta_C)}, \tag{9.3}$$

where v denotes the normalised valuation on K. We thus see that Conjecture 1.7 for C and L/K is equivalent to the assertion

$$\mathfrak{f}(J/K) \stackrel{?}{\equiv} v(\Delta_C) + \dim H^1(k_L/k, \Phi(k_L)) + \epsilon(C/K) + \epsilon(C^L/K) \pmod{2}. \tag{9.4}$$

Since $\mathfrak{f}(J/K)$ and v are unchanged under unramified extension, this predicts that the quantity

$$\dim H^1(k_L/k, \Phi(k_L)) + \epsilon(C/K) + \epsilon(C^L/K) \pmod{2} \tag{9.5}$$

is unchanged upon replacing K by a finite unramified extension F, and replacing L by the unique quadratic unramified extension F'/F. In fact, we can use this observation to predict a simpler expression for (9.5). We begin with some notation.

Notation 9.6. Denote by $\mathcal{C}$ the minimal regular model of C over $\mathcal{O}_K$. For each irreducible component Γ of $\mathcal{C}_{\bar{k}}$, write $d(\Gamma)$ for its multiplicity. Further, denote by ι the automorphism of $\mathcal{C}_{\bar{k}}$ induced from the hyperelliptic involution on C (which extends to an automorphism of $\mathcal{C}$ by uniqueness of the minimal regular model). We then define

$$
\eta(C) = \begin{cases} 1 & g \text{ even and } |\mathrm{orb}_\iota(\Gamma)| \cdot d(\Gamma) \equiv 0 \pmod 2 \text{ for each irreducible component } \Gamma \text{ of } \mathcal{C}_{\bar{k}}, \\ 0 & \text{otherwise,} \end{cases}
$$

where here $\mathrm{orb}_\iota(\Gamma)$ denotes the orbit of an irreducible component Γ under the action of ι.

Now suppose that F/K is a sufficiently large even-degree unramified extension so that G_{k_F} acts trivially on both $\Phi(\bar{k})$ and on the set of irreducible components of $\mathcal{C}_{\bar{k}}$. Let F'/F be the unique quadratic unramified extension. Then we have

$$
H^1(k_{F'}/k_F, \Phi(k_{F'})) \cong \Phi(\bar{k})[2], \qquad \epsilon(C/F) = 0 \quad \text{and} \quad \epsilon(C^{F'}/F) = \eta(C). \qquad (9.7)
$$

The first equality follows from our assumptions on the G_{k_F}-action on $\Phi(\bar{k})$, along with the description of the cohomology of cyclic groups given in [1, Section 8]. The second equality follows from Lemma 6.4 since F/K is assumed to have even degree. The third equality follows from Lemma 6.11, our assumptions on the G_{k_F}-action on the irreducible components of $\mathcal{C}_{\bar{k}}$, and the fact that the formation of the minimal regular model commutes with unramified base change. Indeed, this last fact allows us to identify the geometric special fibre of the minimal regular model of C^L/K with that of C/K, save with G_k-action twisted by ι.

From (9.7), we find

$$
\dim H^1(k_{F'}/k_F, \Phi(k_{F'})) + \epsilon(C/F) + \epsilon(C^{F'}/F) = \dim \Phi(\bar{k})[2] + \eta(C).
$$

Consequently, the discussion preceding Notation 9.6 predicts the following identity, which we will give an unconditional proof of.

Proposition 9.8. *With the notation above, we have*

$$
\dim H^1(k_L/k, \Phi(k_L)) + \epsilon(C/K) + \epsilon(C^L/K) \equiv \dim \Phi(\bar{k})[2] + \eta(C) \pmod 2.
$$

The proof of Proposition 9.8 that we will give is somewhat lengthy and we postpone it to the next section.

An immediate corollary of Proposition 9.8 is the following.

Corollary 9.9. *Conjecture 1.7 holds for C/K and the extension L/K if and only if*

$$
\mathfrak{f}(J/K) \equiv v(\Delta_C) + \dim \Phi(\bar{k})[2] + \eta(C) \pmod 2. \qquad (9.10)
$$

Proof. Combine (the discussion surrounding) (9.4) with Proposition 9.8. □

Remark 9.11. In the statement of Proposition 9.8, it is not simply true that

$$\dim H^1(k_L/k, \Phi(k_L)) \equiv \dim \Phi(\bar{k})[2] \pmod{2}$$

and

$$\epsilon(C/K) + \epsilon(C^L/K) \equiv \eta(C) \pmod{2},$$

as the following example shows.

Example 9.12. Consider the genus 2 hyperelliptic curve

$$C/\mathbb{Q}_3 : y^2 = (x^2 + 3)((x - i)^2 - 3^2)((x + i)^2 - 3^2),$$

where i is a square root of -1. Reducing the defining equation modulo 3 gives a semistable curve. In fact, the above equation viewed as a scheme over $\mathbb{Z}_3$, along with the usual chart at infinity, gives the stable model of C. After base changing to $\mathbb{Z}_3^{\mathrm{nr}}$, its special fibre consists of two rational curves, intersecting transversally at the three points $(0,0)$, $(i, 0)$ and $(-i, 0)$. The final two intersection points are swapped by the Frobenius element $F \in G_k$, whilst the hyperelliptic involution $\iota : (x, y) \mapsto (x, -y)$ fixes each intersection point but swaps the two components. The minimal proper regular model of C over $\mathbb{Z}_3^{\mathrm{nr}}$ is obtained by blowing up once each at the intersection points $(i, 0)$ and $(-i, 0)$. Its special fibre, along with the actions of F and ι, is thus as pictured:
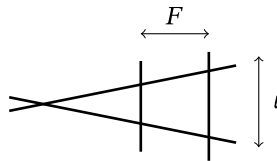
Here, each component pictured is a rational curve of multiplicity 1. Write $L = \mathbb{Q}_3(i)$ for the unique unramified quadratic extension of $\mathbb{Q}_3$. Since F fixes the two components drawn horizontally, we see from Lemma 6.11 that $\epsilon(C/\mathbb{Q}_3) = 0$. Similarly, we have $\eta(C) = 0$ since ι fixes the two components drawn vertically. However, each $\iota \circ F$-orbit of components has size 2, so appealing to Lemma 6.11 once more, we find $\epsilon(C^L/\mathbb{Q}_3) = 1$. Thus,

$$\epsilon(C/K) + \epsilon(C^L/K) \not\equiv \eta(C) \pmod{2}.$$

However, one can also show (e.g. using the description of $\Phi(\bar{k})$ detailed later in Section 10.1) that $\Phi(\bar{k}) \cong \mathbb{Z}/8\mathbb{Z}$ with F acting as multiplication by 5. Thus, we have

$$\dim \Phi(\bar{k})[2] = 1 \quad \text{and} \quad \dim H^1(k_L/k, \Phi(k_L)) = 0.$$

In particular, Proposition 9.8 holds in this example, even though neither of the individual congruences in Remark 9.11 holds.

9.1 | Establishing Equation 9.10 in odd residue characteristic

Assume that the residue characteristic of K is odd. Under this assumption, we now establish the congruence Equation 9.10.

Lemma 9.13. *We have*

$$\mathfrak{f}(J/K) = \mathfrak{f}(J[2]) + \dim \Phi(\bar{k})[2],$$

where here $\mathfrak{f}(J[2])$ denotes the Artin conductor of the G_K-module $J[2]$.

Proof. This is observed by Česnavičius in [9, Lemma 4.2] (we remark that the cited result uses the assumption that K has odd residue characteristic). $\square$

In light of Lemma 9.13, to establish Equation 9.10, it remains to show that

$$\mathfrak{f}(J[2]) \equiv v(\Delta_C) + \eta(C) \pmod 2. \tag{9.14}$$

Fix a Weierstrass equation $C/K : y^2 = f(x)$ for C, where $f(x) \in K[x]$ is a squarefree polynomial. After a change of variables to ensure that the resulting 'x-coordinate' morphism from C to $\mathbb{P}^1$ is unramified over the point at infinity, we can assume that $f(x)$ has even degree $2g + 2$. Let E/K^{nr} be the field extension $E = K^{\mathrm{nr}}(J[2])$, and set $G = \mathrm{Gal}(E/K^{\mathrm{nr}})$. As explained in Section 5, E coincides with the splitting field of $f(x)$ over K^{nr} (recall that we are assuming $g \geqslant 2$). Let $G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots$ be the ramification filtration on G, and write $g_i = |G_i|$. Thus, G_1 is the wild inertia group of E/K^{nr} and is a p-group where $p = \mathrm{char}(k)$ (so, in particular, has odd order), and G/G_1 is cyclic. Let $\mathcal{R}$ denote the G-set of roots of $f(x)$ in E. By definition, we have

$$\mathfrak{f}(J[2]) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} \mathrm{codim}_{\mathbb{F}_2} J[2]^{G_i},$$

the codimension being taken in $J[2]$.

Notation 9.15. With $f(x) \in K[x]$ as above, define $\eta(f) \in \{0, 1\}$ to be equal to 1 if the genus g of C is even and each irreducible factor of $f(x)$ over K^{nr} has even degree. Otherwise, set $\eta(f) = 0$.

Lemma 9.16. *Let $V = \mathbb{C}[\mathcal{R}]$ be the complex permutation representation of G associated to the set of roots of $f(x)$. Then we have*

$$\mathfrak{f}(J[2]) \equiv \mathfrak{f}(V) + \eta(f) \pmod 2.$$

Proof. This will follow from the definitions of $\mathfrak{f}(J[2])$ and $\mathfrak{f}(V)$, along with a comparison between $\mathrm{codim}_{\mathbb{C}} V^{G_i}$ and $\mathrm{codim}_{\mathbb{F}_2} J[2]^{G_i}$ for each i (afforded by Lemma 5.3).

First let $i \geqslant 1$ so that G_i has odd order. Then necessarily, $f(x)$ has an odd degree factor over E^{G_i}, so it follows from Lemma 5.3 that $\dim_{\mathbb{F}_2} J[2]^{G_i} = \dim_{\mathbb{C}} V^{G_i} - 2$. Since also

$\dim_{\mathbb{F}_2} J[2] = \dim_{\mathbb{C}} V - 2$, we see that

$$\sum_{i=1}^{\infty} \frac{g_i}{g_0} \operatorname{codim}_{\mathbb{F}_2} J[2]^{G_i} = \sum_{i=1}^{\infty} \frac{g_i}{g_0} \operatorname{codim}_{\mathbb{C}} V^{G_i}.$$

It remains to show that

$$\operatorname{codim}_{\mathbb{F}_2} J[2]^G \equiv \operatorname{codim}_{\mathbb{C}} V^G + \eta(f) \pmod{2}.$$

When g is even, Lemma 5.3 gives $\dim_{\mathbb{F}_2} J[2]^G = \dim_{\mathbb{C}} V^G - 2 + \eta(f)$ and we are done. So, suppose that g is odd. If $f(x)$ has an odd degree factor over K^{nr}, then again, we conclude immediately from Lemma 5.3. Finally, suppose that each irreducible factor of $f(x)$ over K^{nr} has even degree. Write $f(x) = c_f f_0(x)$ where c_f is the leading coefficient of $f(x)$ and $f_0(x)$ is monic. Applying Lemma 5.3, once again it suffices to show that there is a unique quadratic subextension of E/K^{nr} over which $f_0(x)$ factors into two distinct, conjugate polynomials. To see this, firstly note that there is a unique quadratic subextension of E/K^{nr}. Indeed, any such extension must necessarily be contained in E^{G_1}, and E^{G_1}/K^{nr} is cyclic and (by the assumption on the degrees of the irreducible factors of $f(x)$ over K^{nr}) has even degree. To see that $f_0(x)$ admits the required factorisation over this extension, let $S = \{h_1, \dots, h_l\}$ be the set of irreducible factors of $f_0(x)$ over E^{G_1}, each of which necessarily has odd degree. The cyclic group G/G_1 acts on S and since each factor of $f_0(x)$ over K^{nr} has even degree, each orbit of G/G_1 on S has even order. Denote these disjoint orbits by $S_1, \dots, S_t$, and for $1 \leqslant i \leqslant t$, write $S_i = \{h_{i,1}(x), \dots, h_{i,d_i}(x)\}$. Fix a generator σ of G/G_1 and assume without loss of generality that $\sigma h_{i,j}(x) = h_{i,j+1 (\mathrm{mod}\ d_i)}(x)$. Then the polynomial

$$h(x) = \prod_{i=1}^{t} \prod_{j\ \mathrm{odd}} h_{i,j}(x)$$

is fixed by σ^2, has $\sigma h(x) \neq h(x)$ and is such that $f_0(x) = h(x) \cdot \sigma h(x)$. □

Next, we relate the Artin conductor of $V = \mathbb{C}[\mathcal{R}]$ to the discriminant Δ_f of $f(x)$.

Lemma 9.17. *Let $V = \mathbb{C}[\mathcal{R}]$ be as above. Then*

$$\mathfrak{f}(V) \equiv v(\Delta_f) \pmod 2.$$

Proof. Write $f(x) = f_1(x) \dots f_t(x)$ as a product of irreducible polynomials over K, and write $\mathcal{R}_i$ for the set of roots of $f_i(x)$ in E. Then V is a direct sum of the permutation modules $V_i = \mathbb{C}[\mathcal{R}_i]$, so $\mathfrak{f}(V)$ is the sum of the $\mathfrak{f}(V_i)$. Further, since for polynomials h_1, h_2, we have $\Delta_{h_1 h_2} = \Delta_{h_1} \Delta_{h_2} \operatorname{Res}(h_1, h_2)^2$ (here $\operatorname{Res}(h_1, h_2)$ denotes the resultant of h_1, h_2), we see that the discriminant of $f(x)$ is, up to squares in K, the product of the discriminants of the $f_i(x)$. In this way, we reduce to the case where $f(x)$ is irreducible, which we treat now.

Assuming that $f(x)$ is irreducible, let F/K be the splitting field of $f(x)$ and let H be the stabiliser in $\operatorname{Gal}(F/K)$ of a root $r \in \mathcal{R}$. Then $V \cong \mathbb{C}[\operatorname{Gal}(F/K)/H]$, so by the conductor-discriminant formula [57, VI.2 corollary to Proposition 4], we have $\mathfrak{f}(V) = v(\Delta_{F^H/K})$, where $\Delta_{F^H/K}$ denotes the discriminant of F^H/K. Since $F^H = K(r)$, we have $v(\Delta_{F^H/K}) \equiv v(\Delta_f) \pmod 2$, as desired. □

Combined, 9.16, 9.17 establish the congruence

$$\mathfrak{f}(J[2]) \equiv v(\Delta_f) + \eta(f) \pmod{2}. \tag{9.18}$$

To prove Equation 9.10, it remains to reinterpret the 'correction' term $\eta(f)$.

Lemma 9.19. *Let F/K be a finite unramified extension and denote by F'/F the unique quadratic unramified extension of F. Then, provided that F/K is sufficiently large, we have $\eta(f) = \epsilon(C^{F'}/F)$. In particular, we have $\eta(f) = \eta(C)$.*

Proof. Arguing as in the proof of Lemma 9.16, we see that $f(x)$ either has an odd degree factor over K^{nr}, or factors as a product of two conjugate polynomials over the unique quadratic extension of K^{nr} (whilst this is shown in the proof of Lemma 9.16 under a running assumption that g is odd, the argument given there works verbatim when g is even also). From this, we deduce that for every sufficiently large unramified extension F/K, either $f(x)$ has an odd degree factor over F, or $f(x)$ factors as a product of two conjugate polynomials over some totally ramified quadratic extension L/F (the latter happening if and only if each irreducible factor of $f(x)$ over K^{nr} has even degree). In the latter case, by enlarging F/K further if necessary we may also assume that the leading coefficient of $f(x)$ is a norm from this quadratic extension. Since the quadratic twist $C^{F'}/F$ is given by the equation $C^{F'} : y^2 = uf(x)$ where u is a non-square unit in F, the claim that $\eta(f) = \epsilon(C^{F'}/F)$ follows from Proposition 6.7 and the fact that $(u, L/F) = -1$. That $\eta(f) = \eta(C)$ now follows from (9.7). $\qquad\square$

Corollary 9.20. *Under the assumption that K has odd residue characteristic, (9.10) holds for C.*

Proof. Lemma 9.19 allows us to replace $\eta(f)$ with $\eta(C)$ in (9.18), hence establishing (9.14). Combining this with Lemma 9.13 gives the result. $\qquad\square$

9.2 | Residue characteristic 2

We now give certain conditions under which the congruence (9.10) holds (or rather, can be shown to hold) when the residue characteristic of K is 2. Thus, for the rest of this subsection, we assume that K is a finite extension of $\mathbb{Q}_2$.

9.2.1 | Good reduction of the Jacobian

If the Jacobian J/K of C has good reduction, then we have

$$\mathfrak{f}(J/K) = 0 \quad \text{and} \quad \Phi(\bar{k}) = 0. \tag{9.21}$$

Moreover, we have the following.

Proposition 9.22. *Under the assumption that J/K has good reduction, we have*

$$v(\Delta_C) \equiv 0 \pmod{2}.$$

Proof. Let $\mathcal{J}/\mathcal{O}_K$ be the Néron model of J. The assumption that J has good reduction over K implies that $\mathcal{J}[2]$ is a finite flat group scheme over $\mathcal{O}_K$ [39, Proposition 20.7]. Letting e denote the absolute ramification index of K, it is a theorem of Fontaine that G_K^u acts trivially on $\mathcal{J}[2](\bar{K}) = J[2]$ provided $u > 2e - 1$ [21, Théorème A]. Note that we are using Serre's upper numbering for the higher ramification groups. Let $F = K(\sqrt{\Delta_C})$ and $G = \mathrm{Gal}(F/K)$, noting that $F \subseteq K(J[2])$. Combining the above discussion with Herbrand's theorem (see, e.g. [57, IV, Lemma 3.5]), we see that G^u is trivial for $u \geqslant 2e$. In particular, the conductor of F/K, which we denote $\mathfrak{f}(F/K)$, satisfies $\mathfrak{f}(F/K) \leqslant 2e$.

Now suppose, for contradiction, that $v(\Delta_C)$ is odd. We thus have $F = K(\sqrt{\pi})$ for some uniformiser π of K. Letting σ denote the non-trivial element of G, this gives

$$v_F\left(\sigma\left(\sqrt{\pi}\right) - \sqrt{\pi}\right) = v_F(2) + 1 = 2e + 1,$$

where v_F denotes the normalised valuation on F. From this, we obtain $\mathfrak{f}(F/K) = 2e + 1$, contradicting the bound above. Thus, $v(\Delta_C)$ is even. $\qquad\square$

Remark 9.23. This proposition is trivially true also if J has good reduction and the residue characteristic of K is odd. Indeed, then $J[2]$ is unramified, so Δ_C is a square in K^{nr}. In particular, Δ_C has even valuation.

Lemma 9.24. *Under the assumption that J/K has good reduction, we have $\eta(C) = 0$.*

Proof. Let $\mathcal{C}/\mathcal{O}_K$ denote the minimal regular model of C. Since J has good reduction, the curve C/K is semistable and the dual graph of $\mathcal{C}_{\bar{k}}$ is a tree [29, Proposition 10.1.51].[†] Moreover, as there are no exceptional curves in $\mathcal{C}_{\bar{k}}$, each leaf corresponds to a positive genus component (which necessarily has multiplicity 1). Since the quotient of $\mathcal{C}_{\bar{k}}$ by the hyperelliptic involution has arithmetic genus zero, the hyperelliptic involution necessarily fixes every leaf, and hence acts trivially on the dual graph. $\qquad\square$

Corollary 9.25. *If J/K has good reduction, then (9.10) holds for C.*

Proof. Combine (9.21) with Proposition 9.22 and Lemma 9.24. $\qquad\square$

9.2.2 | Semistable curves of genus 2

When the genus of C is 2, we can draw on results of Liu [30] to establish additional cases of (9.10).

Proposition 9.26. *Suppose that C/K is semistable and has genus 2. Then (9.10) holds for C.*

Proof. This follows from Liu's genus 2 version of Ogg's formula [30, Theorem 1]. Specifically, combining Theorem 1, Theorem 2 and Proposition 1 of [30], one obtains (independently of the

---

[†] By definition, the dual graph of $\mathcal{C}_{\bar{k}}$ is the finite connected graph with a vertex for each irreducible component of $\mathcal{C}_{\bar{k}}$, and such that vertices corresponding to components Γ_1 and Γ_2 are joined by one edge for each ordinary double point of $\mathcal{C}_{\bar{k}}$ lying on both Γ_1 and Γ_2.

residue characteristic of K)

$$\mathfrak{f}(J/K) \equiv v(\Delta_C) + n - 1 + \frac{d-1}{2} \pmod 2,$$

where n is the number of irreducible components of $C_{\bar{k}}$ (as usual C denotes the minimal regular model of C over $\mathcal{O}_K$) and where d is defined in the statement of Liu's Theorem 1. In [30, Section 5.2], Liu computes the term $\frac{d-1}{2}$ in a large number of cases, though not all in residue characteristic 2, in terms of the structure of $C_{\bar{k}}$ (more specifically, in terms of the 'type' of $C_{\bar{k}}$ as classified in [43] and [47]). This includes in particular all cases where C/K has semistable reduction. It is then easy to establish Equation 9.10 for all semistable curves of genus 2 by combining this with the description, detailed in [31, Section 8], of the component group of a genus 2 curve in terms of its type. □

9.3 | Proof of Proposition 9.1

The above results combine to prove Proposition 9.1, conditional on the soon to be proven Proposition 9.8.

Proof of Proposition 9.1 (Conditional on Proposition 9.8). Combine Corollary 9.9 with Corollary 9.20 in Case (i), Corollary 9.25 in Case (ii) and Proposition 9.26 in Case (iii). □

10 | THE PROOF OF PROPOSITION 9.8

Maintaining the setup of the previous section, we now turn to proving Proposition 9.8. We will deduce this from Theorem 10.2. This is a result applying to arbitrary curves, and which may be of independent interest. We begin by recalling a well-known description of the component group $\Phi(\bar{k})$ of the Jacobian of a (not necessarily hyperelliptic) curve in terms of its minimal regular model.

10.1 | The component group via the minimal regular model

See [5, Section 1] and [6, Chapter 9] for details of what follows. Let X be a smooth, proper, geometrically connected curve of genus g over K, let $\mathcal{X}/\mathcal{O}_K$ be its minimal proper regular model and let $\mathcal{X}_{\bar{k}}$ denote the special fibre of $\mathcal{X}$, base-changed to $\bar{k}$. Let $\{\Gamma_i\}_{i \in I}$ be the set of irreducible components of $\mathcal{X}_{\bar{k}}$. For each $i \in I$, denote by d_i the multiplicity of Γ_i. Let $\mathbb{Z}^I$ denote the free $\mathbb{Z}$-module on the Γ_i's and define $\alpha : \mathbb{Z}^I \to \mathbb{Z}^I$ by

$$\alpha(D) = \sum_{i \in I} (D \cdot \Gamma_i)\Gamma_i,$$

where $D \cdot \Gamma_i$ is the intersection number between D and Γ_i. Further, define $\beta : \mathbb{Z}^I \to \mathbb{Z}$ by setting $\beta(\Gamma_i) = d_i$ and extending linearly. The natural action of G_k on $\mathcal{X}_{\bar{k}}$ makes $\mathbb{Z}^I$ into a G_k-module, and α is equivariant for this action. Endowing $\mathbb{Z}$ with trivial G_k-action, the same is true of β. In this way, both $\mathrm{im}(\alpha)$ and $\ker(\beta)$ become G_k-modules.

Let J/K be the Jacobian of X, and denote by Φ its Néron component group. As explained in [5, Theorem 1.1], by work of Raynaud, we have an exact sequence of G_k-modules

$$0 \longrightarrow \mathrm{im}(\alpha) \longrightarrow \ker(\beta) \longrightarrow \Phi(\bar{k}) \longrightarrow 0. \tag{10.1}$$

Denoting by $F \in G_k$ the Frobenius element, we thus have

$$\left| \Phi(k) \right| = \left| (\ker(\beta)/\mathrm{im}(\alpha))^F \right|.$$

Note that F acts on $\mathbb{Z}^I$ as a permutation of I, commuting with α and β, and preserving the arithmetic genus of components.

We recall also from Lemma 6.11 that X is deficient over K if and only if

$$\gcd_{i\in I}\{d_i \cdot |\mathrm{orb}_F(\Gamma_i)|\}$$

does not divide $g - 1$, where $\mathrm{orb}_F(\Gamma_i)$ denotes the F-orbit of Γ_i (for the application of Lemma 6.11, note that since F topologically generates G_k and $\mathcal{X}_{\bar{k}}$ has only finitely many irreducible components, we have $\mathrm{orb}_F(\Gamma_i) = \mathrm{orb}_{G_k}(\Gamma_i)$ for every $i \in I$).

10.2 | The result for general curves: Statement

Maintaining the notation of the previous subsection, denote by $\mathfrak{G}$ the group of all permutations of I commuting with the maps α and β and preserving the arithmetic genus of components. By assumption, $\mathfrak{G}$ acts on $\mathrm{im}(\alpha)$ and $\ker(\beta)$. Via the sequence (10.1), we have an induced action of $\mathfrak{G}$ on $\Phi(\bar{k})$. For $\sigma \in \mathfrak{G}$, we define

$$q(\sigma) = \begin{cases} 1 & \gcd_{i\in I}\{d_i \cdot |\mathrm{orb}_\sigma(\Gamma_i)|\} \text{ divides } g - 1, \\ 2 & \text{otherwise.} \end{cases}$$

In particular, viewing the Frobenius $F \in G_k$ as an element of $\mathfrak{G}$, we have $q(F) = 2^{\epsilon(X/K)}$.

We will obtain Proposition 9.8 as a consequence of the following.

Theorem 10.2. *Let $\mathfrak{G}$ be as above. Then, the map $D : \mathfrak{G} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ defined by*

$$D(\sigma) = q(\sigma) \cdot \frac{\left| \Phi(\bar{k}) \right|}{\left| \Phi(\bar{k})^\sigma \right|}$$

is a homomorphism.

Before proving Theorem 10.2, we explain how to use it to deduce Proposition 9.8.

10.3 | Deducing Proposition 9.8 from Theorem 10.2

Proof of Proposition 9.8 (conditional on Theorem 10.2). Maintaining the notation above, suppose $X = C$ is a hyperelliptic curve over K. The hyperelliptic involution ι of C extends to an

automorphism of the minimal regular model of C, and may therefore be viewed as an element of $\mathfrak{G}$. Moreover, as the induced automorphism ι_* of the Jacobian of C is multiplication by -1, the action on Φ induced by ι is multiplication by -1 also (cf. proof of [5, Theorem 1.1]). Thus,

$$\Phi(\bar{k})[2] = \Phi(\bar{k})^\iota.$$

Let L denote the unique quadratic unramified extension of K and, as usual, denote by F the Frobenius element in G_k. Then, we have

$$\left|H^1(k_L/k, \Phi(k_L))\right| = \left|\frac{\ker\left(1 + F|\Phi(\bar{k})^{F^2}\right)}{\mathrm{im}\left(1 - F|\Phi(\bar{k})^{F^2}\right)}\right| = \frac{\left|\Phi(\bar{k})^{\iota \circ F}\right| \cdot \left|\Phi(\bar{k})^F\right|}{\left|\Phi(\bar{k})^{F^2}\right|}.$$

Here, for the first equality, we are using the description of the cohomology of cyclic groups given in [1, Section 8].

From Lemma 6.4, we have $\epsilon(C/L) = 0$, hence $q(F^2) = 1$. Moreover, we have $\eta(C) = \mathrm{ord}_2\, q(\iota)$, $\epsilon(C/K) = \mathrm{ord}_2\, q(F)$, and $\epsilon(C^L/K) = \mathrm{ord}_2\, q(\iota \circ F)$. To obtain the last equality, we note that, since the formation of minimal regular models commutes with unramified base change, we may identify the geometric special fibre of the minimal regular model of C^L/K with that of C/K, save with G_k-action twisted by the hyperelliptic involution.

On the other hand, it follows from Theorem 10.2 that

$$D(F)D(\iota \circ F)D(F^2) = D(\iota)$$

as elements of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Taking 2-adic valuations of this equation, and interpreting the resulting terms via the discussion above, we obtain the congruence of Proposition 9.8. □

10.4 | Proof of Theorem 10.2

In what follows we take the notation introduced in the statement of Theorem 10.2.

Lemma 10.3. *For each $\sigma \in \mathfrak{G}$, we have*

$$D(\sigma) = \left|\det\left(\alpha|(\sigma - 1)\mathbb{Q}^I\right)\right|.$$

(That is, as elements of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, $D(\sigma)$ is the absolute value of the determinant of α viewed as an endomorphism of $(\sigma - 1)\mathbb{Q}^I$.)

Proof. Fix $\sigma \in \mathfrak{G}$, define $d = \gcd_{i \in I}\{d_i\}$ and $d'(\sigma) = \gcd_{i \in I}\{|\mathrm{orb}_\sigma(\Gamma_i)| \cdot d_i\}$. By [5, Proof of Theorem 1.17], we have

$$\left|\Phi(\bar{k})^\sigma\right| \cdot q(\sigma) = \left|\frac{\ker(\beta)^\sigma}{\mathrm{im}(\alpha)^\sigma}\right| \cdot \frac{d'(\sigma)}{d}.$$

We remark that, in order to apply the cited result, we are using the assumption that $\mathfrak{G}$ preserves the arithmetic genus of components.

In what follows, to ease notation, we write Λ for the $\mathbb{Z}[\mathfrak{G}]$-module $\mathbb{Z}^I$. Now

$$\ker(\beta)^\sigma / \mathrm{im}(\alpha)^\sigma \cong \ker\left(\beta : \Lambda^\sigma / \mathrm{im}(\alpha)^\sigma \longrightarrow d'(\sigma)\mathbb{Z}\right).$$

We now apply the snake lemma to the commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \dfrac{\Lambda^\sigma}{\mathrm{im}(\alpha)^\sigma} & \longrightarrow & \dfrac{\Lambda}{\mathrm{im}(\alpha)} & \longrightarrow & \dfrac{\Lambda}{\mathrm{im}(\alpha) + \Lambda^\sigma} & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle\beta_1} & & \downarrow{\scriptstyle\beta_2} & & \downarrow{\scriptstyle\beta_3} & & \\
0 & \longrightarrow & d'(\sigma)\mathbb{Z} & \longrightarrow & d\mathbb{Z} & \longrightarrow & d\mathbb{Z}/d'(\sigma)\mathbb{Z} & \longrightarrow & 0,
\end{array}
$$

where each vertical arrow is induced by β. Noting that all vertical arrows are surjective, this gives

$$D(\sigma) = \frac{dq(\sigma)^2}{d'(\sigma)} |\ker(\beta_3)| = q(\sigma)^2 \frac{d^2}{d'(\sigma)^2} \left| \frac{\Lambda}{\mathrm{im}(\alpha) + \Lambda^\sigma} \right|.$$

Thus, as a function $\mathfrak{G} \to \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$, we have

$$D(\sigma) = \left| \frac{\Lambda}{\mathrm{im}(\alpha) + \Lambda^\sigma} \right|.$$

Now $\sigma - 1$ induces an isomorphism

$$\frac{\Lambda}{\mathrm{im}(\alpha) + \Lambda^\sigma} \xrightarrow{\ \sim\ } \frac{(\sigma - 1)\Lambda}{(\sigma - 1)\alpha(\Lambda)} = \frac{(\sigma - 1)\Lambda}{\alpha((\sigma - 1)\Lambda)},$$

where for the last equality, we use that σ commutes with α.

To conclude, note that $(\sigma - 1)\Lambda$ is a free $\mathbb{Z}$-module of finite rank, and α is a linear endomorphism of this group. By properties of Smith normal form, the order of the group

$$\frac{(\sigma - 1)\Lambda}{\alpha((\sigma - 1)\Lambda)}$$

is equal to the absolute value of the determinant of α as an endomorphism of the $\mathbb{Q}$-vector space $(\sigma - 1)\mathbb{Q}^I$. This gives the result. $\qquad\square$

The passage from $\mathbb{Z}[\mathfrak{G}]$-modules to $\mathbb{Q}[\mathfrak{G}]$-modules provided by Lemma 10.3 allows us to make use of representation theory in characteristic zero. Note that the matrix representing α on $\mathbb{Q}^I$ with respect to the natural permutation basis is symmetric (it is just the intersection matrix associated to $\mathcal{X}_{\bar{k}}$). We thus see that the minimal polynomial of α as an endomorphism of $\mathbb{Q}^I$ splits over $\mathbb{R}$. Moreover, the kernel of α is $\left(\sum_{i \in I} d_i \Gamma_i\right) \cdot \mathbb{Q}$, which is fixed by $\mathfrak{G}$. These observations motivate (and allow us to apply) the following lemmas.

Lemma 10.4. *Let G be a finite cyclic group with generator σ, and let V be a $\mathbb{Q}[G]$-representation. Let $\alpha \in End_{\mathbb{Q}[G]}V$ be a G-endomorphism of V whose minimal polynomial splits over $\mathbb{R}$ and is such*

that $\ker(\alpha) \subseteq V^G$. *Then*

$$\det\left(\alpha|(\sigma-1)V\right) \equiv \det\left(\alpha|V_{-1,\sigma}\right) (mod \ \mathbb{Q}^{\times 2}),$$

where $V_{-1,\sigma}$ is the (-1)-eigenspace for σ on V.

Proof. Let $V = \bigoplus_{i=1}^{n} V_i^{d_i}$ be an isotypic decomposition of V, so that each V_i is an irreducible $\mathbb{Q}[G]$-representation and $V_i \not\cong V_j$ for $i \neq j$. Suppose, without loss of generality, that V_1 is the trivial representation. Now α preserves this decomposition and $(\sigma-1)V = \bigoplus_{i=2}^{n} V_i^{d_i}$. Since $\ker(\alpha) \subseteq V^G$, the restriction of α to each $V_i^{d_i}$ is non-singular. Thus, we reduce to the case where α is non-singular and $V = W^d$ for an irreducible non-trivial $\mathbb{Q}[G]$-representation W. Let χ be the character of a complex irreducible constituent of W. We can suppose that χ is non-real (so that $\chi(\sigma) \notin \{\pm 1\}$), in which case we wish to show that $\det(\alpha) \in \mathbb{Q}^{\times 2}$. Now $\mathrm{End}_{\mathbb{Q}[G]}V \cong \mathrm{Mat}_d(\mathrm{End}_{\mathbb{Q}[G]}W)$ is a finite-dimensional simple algebra over $\mathbb{Q}$. Set $D = \mathrm{End}_{\mathbb{Q}[G]}W$ so that D is a division algebra, and let $K/\mathbb{Q}$ be the centre of D. We have $K \cong \mathbb{Q}(\chi)$ as $\mathbb{Q}$-algebras, where $\mathbb{Q}(\chi)$ is the character field of χ. See, for example, [53] for proofs of the representation-theoretic facts used above. Note that $K/\mathbb{Q}$ is abelian.

Now via the diagonal embedding of K into $\mathrm{End}_{\mathbb{Q}[G]}V$, V becomes a $K[G]$-module. Since K is the centre of $\mathrm{End}_{\mathbb{Q}[G]}V$, each $\mathbb{Q}[G]$-endomorphism of V is in fact K-linear, so we may view α as a $K[G]$-endomorphism of V. Denoting $\det_K(\alpha)$ the determinant of α viewed as a K-endomorphism, we have

$$\det(\alpha) = N_{K/\mathbb{Q}}(\det_K(\alpha))$$

(see, e.g. [7, Theorem A.1]).

As χ is assumed non-real, the field K in not totally real, and hence, there is an index 2 totally real subfield K^+ of K (recall that $K/\mathbb{Q}$ is abelian). We claim that $\det(\alpha)$ is in K^+. Indeed, since the minimal polynomial of α as a $\mathbb{Q}$-endomorphism of V splits over $\mathbb{R}$, each root of the minimal polynomial of α as a K-endomorphism of V is totally real. It follows that $\det(\alpha)$ is a product of totally real numbers, hence in K^+. Thus,

$$\det(\alpha) = N_{K/\mathbb{Q}}(\det_K(\alpha)) = N_{K^+/\mathbb{Q}}(\det_K(\alpha))^2 \in \mathbb{Q}^{\times 2}$$

as desired. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad$ $\square$

Lemma 10.5. *Let G be a finite group and V a $\mathbb{Q}[G]$-representation. Let $\alpha \in End_{\mathbb{Q}[G]}V$ be a G-endomorphism of V whose minimal polynomial splits over $\mathbb{R}$ and is such that $\ker(\alpha) \subseteq V^G$. Then the function $\phi : G \to \mathbb{Q}^{\times}/\mathbb{Q}^{\times 2}$ defined by*

$$\phi(\sigma) = det\left(\alpha|V_{-1,\sigma}\right)$$

is a homomorphism.

Proof. Similarly to the proof of Lemma 10.4, by considering an isotypic decomposition of V, we reduce to the case where α is non-singular and $V = W^d$ for some $d \geqslant 1$ and irreducible $\mathbb{Q}[G]$-representation W. As in that proof, let D be the division algebra $D = \mathrm{End}_{\mathbb{Q}[G]}W$ so that $\mathrm{End}_{\mathbb{Q}[G]}V \cong \mathrm{Mat}_d(D)$, let $K/\mathbb{Q}$ be the centre of D and let χ be the character of a complex

irreducible constituent of W. Once again, we have $K \cong \mathbb{Q}(\chi)$, $K/\mathbb{Q}$ is abelian and we may view α as a $K[G]$-endomorphism of V. Moreover, we similarly have

$$\det(\alpha|V_{-1,\sigma}) = N_{K/\mathbb{Q}}(\det_K(\alpha|V_{-1,\sigma}))$$

for all $\sigma \in G$. Denoting by ϕ_K the function $G \to K^\times/K^{\times 2}$ given by

$$\phi_K(\sigma) = \det_K(\alpha|V_{-1,\sigma}),$$

we thus have $\phi = N_{K/\mathbb{Q}} \circ \phi_K$.

First suppose that K is not totally real. Then there is an index 2 totally real subfield K^+ of K. Since the minimal polynomial of α as a $\mathbb{Q}$-endomorphism of V splits over $\mathbb{R}$, $\det_K(\alpha|V_{-1,\sigma})$ lies in K^+. Thus,

$$\phi(\sigma) = N_{K/\mathbb{Q}} \circ \phi_K(\sigma) = \left(N_{K^+/\mathbb{Q}} \circ \phi_K(\sigma)\right)^2 \in \mathbb{Q}^{\times 2},$$

hence ϕ is trivial in this case.

Now assume that K is totally real, or equivalently that χ is real valued. Let m be the Schur index of χ (over $\mathbb{Q}$ or equivalently K). Suppose first that χ is realisable over $\mathbb{R}$. Then, via a chosen embedding $K \hookrightarrow \mathbb{R}$, we have $V \otimes_K \mathbb{R} \cong U^{md}$ for some absolutely irreducible real representation U. Fix $\sigma \in G$. Then $V_{-1,\sigma} \otimes_K \mathbb{R} = (V \otimes_K \mathbb{R})_{-1,\sigma} = (U_{-1,\sigma})^{md}$. View α as a matrix $M \in \mathrm{Mat}_{md}(\mathbb{R})$ via the identification $\mathrm{End}_{\mathbb{R}[G]}(U^{md}) \cong \mathrm{Mat}_{md}(\mathrm{End}_{\mathbb{R}[G]} U) = \mathrm{Mat}_{md}(\mathbb{R})$. The determinant of α, viewed as a K-endomorphism of $(U_{-1,\sigma})^{md}$, is then equal to $\det(M)^{\dim U_{-1,\sigma}}$. In fact, one sees that $\det(M)$ is equal to $\mathrm{Nrd}(\alpha) \in K^\times$ where here Nrd denotes the reduced norm on the central simple algebra $A = \mathrm{End}_{\mathbb{Q}[G]} V$ over K.

We claim that the congruence

$$\dim U_{-1,\sigma} + \dim U_{-1,\tau} \equiv \dim U_{-1,\sigma\tau} \pmod 2 \tag{10.6}$$

holds for all σ and τ in G. Combined with the above discussion, this shows that ϕ_K, hence ϕ, is a homomorphism in this case. To prove the claim, we note that U is a real vector space and each $\sigma \in G$ acts on U as a finite order matrix N_σ which is hence diagonalisable over $\mathbb{C}$. Base-changing to $\mathbb{C}$, diagonalising N_σ and noting that the eigenvalues of N_σ are roots of unity appearing in complex-conjugate pairs, one sees that for each $\sigma \in G$, we have

$$(-1)^{\dim U_{-1,\sigma}} = \det(N_\sigma).$$

The congruence (10.6) now follows from multiplicativity of the determinant.

Finally, suppose that χ is not realisable over $\mathbb{R}$. Then we have $V \otimes_K \mathbb{C} \cong U^{md}$ where U is an irreducible representation over $\mathbb{C}$ such that U, hence U^{md}, possesses a non-degenerate G-invariant alternating form. Denote by $\langle\,,\,\rangle$ such a form on U^{md}. The argument for the previous case again gives $\det_K(\alpha|V_{-1,\sigma}) = \mathrm{Nrd}(\alpha)^{\dim U_{-1,\sigma}}$. We claim that $\dim U_{-1,\sigma}$ is even for each $\sigma \in G$, from which it follows that ϕ_K, hence ϕ, is trivial. Indeed, the pairing $\langle\,,\,\rangle$ gives a G-equivariant isomorphism from U to its dual U^*. This isomorphism respects the σ-eigenspace decomposition on each side and hence restricts to an isomorphism $U_{-1,\sigma} \xrightarrow{\sim} U^*_{-1,\sigma}$ whose associated bilinear pairing is non-degenerate and alternating. Thus, $\dim U_{-1,\sigma}$ is even. $\qquad\square$

Proof of Theorem 10.2. In the notation of Section 10.1, let V denote the $\mathbb{Q}[\mathfrak{G}]$-representation $\mathbb{Q}^I$. For $\sigma \in \mathfrak{G}$, combining Lemma 10.3 with Lemma 10.4, we see that we have

$$D(\sigma) = \det\left(\alpha | V_{-1,\sigma}\right) \in \mathbb{Q}^\times / \mathbb{Q}^{\times 2}.$$

(That the assumptions of Lemma 10.4 are satisfied follows from the discussion preceding the statement of that lemma.) The result now follows from Lemma 10.5. $\qquad\square$

10.5 | Computing Tamagawa numbers modulo squares

The proof of Theorem 10.2 facilitates the computation of Tamagawa numbers of hyperelliptic curves, at least up to squares, and to end the section, we record this in the following proposition. To make the statement more self-contained, we summarise now the notation used.

Notation 10.7. We take the following notation:

- K a non-archimedean local field,
- X/K a smooth, proper, geometrically connected curve of genus g,
- Φ the Néron component group (scheme) of the Jacobian of X,
- $\mathcal{X}/\mathcal{O}_K$ the minimal proper regular model of X,
- $\mathcal{X}_{\bar{k}}$ the special fibre of $\mathcal{X}$ base-changed to $\bar{k}$,
- $\Gamma_1, \dots, \Gamma_n$ the irreducible components of $\mathcal{X}_{\bar{k}}$, and r_i the size of the G_k-orbit of Γ_i,
- $\epsilon(X/K) \in \{0, 1\}$, defined to be equal to 1 if X is deficient over K, and 0 otherwise,
- F the Frobenius element in G_k.

Proposition 10.8. *Take the notation above. Moreover, let $S_1, \dots, S_t$ be the even-sized orbits of G_k on the set $\{\Gamma_1, \dots, \Gamma_n\}$ of irreducible components. For each $1 \leqslant i \leqslant t$, let $m_i = |S_i|$, let $\Gamma_{i,1}$ be a representative of the orbit S_i and define*

$$\epsilon_i = \sum_{j=0}^{m_j - 1} (-1)^j F^j(\Gamma_{i,1}).$$

Then

$$2^{\epsilon(X/K)} \cdot \frac{|\Phi(\bar{k})|}{|\Phi(k)|} \equiv \left| \det\left(\frac{1}{m_j} \left\langle \epsilon_i, \epsilon_j \right\rangle \right)_{1 \leqslant i,j \leqslant t} \right| \ (\mathrm{mod} \ \mathbb{Q}^{\times 2}),$$

where $\langle \cdot, \cdot \rangle$ denotes the intersection pairing on $\mathcal{X}_{\bar{k}}$.

Proof. Lemma 10.3 combined with Lemma 10.4 gives

$$2^{\epsilon(X/K)} \cdot \frac{|\Phi(\bar{k})|}{|\Phi(k)|} \equiv |\det(\alpha | V_{-1})| \ (\mathrm{mod} \ \mathbb{Q}^{\times 2}), \tag{10.9}$$

where V_{-1} denotes the (-1)-eigenspace of F on the permutation module $V = \mathbb{Q}^I$, and α is the linear map defined from the intersection pairing, as detailed in Section 10.1. Now $\{\epsilon_1, \dots, \epsilon_t\}$ forms

a basis for V_{-1} and, using G_k-invariance of the intersection pairing, for each $1 \leqslant i \leqslant t$, we have

$$\alpha(\epsilon_i) = \sum_{j=1}^{t} \langle \epsilon_i, \Gamma_{j,1} \rangle \epsilon_j = \sum_{j=1}^{t} \frac{1}{m_j} \langle \epsilon_i, \epsilon_j \rangle \epsilon_j.$$

Combined with Equation 10.9, this gives the result. □

11 | RAMIFIED EXTENSIONS IN ODD RESIDUE CHARACTERISTIC: GENERALITIES

Let K be a non-archimedean local field of odd residue characteristic. In this section, we consider Conjecture 1.7 when the quadratic extension L/K is ramified. Specifically, across Sections 11–15, we will prove the following.

Proposition 11.1 (=Proposition 15.1). *Let C/K be a hyperelliptic curve and let L/K be a ramified quadratic extension. If C/K has semistable reduction, then Conjecture 1.7 holds for C and the extension L/K.*

Thus, for this section, we fix a ramified quadratic extension L/K, and fix a hyperelliptic curve C/K with semistable reduction. As usual, we denote by J the Jacobian of C. Recall from Lemma 3.4 that since K has odd residue characteristic, we can express the cokernel of the local norm map in terms of Tamagawa numbers:

$$\dim J(K)/N_{L/K}J(L) = \mathrm{ord}_2 \frac{c(J/K)c(J^L/K)}{c(J/L)}. \tag{11.2}$$

We begin by describing a method for computing the ratio $\frac{c(J/L)}{c(J/K)}$ up to rational squares for general semistable curves. Separately, we will compute $c(J^L/K)$ up to squares by analysing the minimal regular model of the quadratic twist of C by L. Since C^L/K is not semistable, we use results from Section 10 to facilitate this computation. As we shall see, the terms in Conjecture 1.7 involving deficiency and root numbers will naturally appear along the way. For a more precise description of the strategy for proving Proposition 11.1, see Section 11.3 below.

11.1 | The minimal proper regular model of a semistable curve

For proofs and more details of what follows we refer to [23]. For the specific formulation detailed below, we refer to [18, Section 2] and the references therein.

Denote by $\mathcal{C}/\mathcal{O}_K$ the minimal proper regular model of C, and denote by $\mathcal{C}_{\bar{k}}$ the special fibre of $\mathcal{C}$, base-changed to $\bar{k}$. Since C/K is assumed semistable, $\mathcal{C}_{\bar{k}}$ is a semistable curve over $\bar{k}$. Let Y_C denote the dual graph $\mathcal{C}_{\bar{k}}$; by definition, this is the finite connected graph with a vertex for each irreducible component of $\mathcal{C}_{\bar{k}}$, and such that vertices corresponding to components Γ_1 and Γ_2 are joined by one edge for each ordinary double point of $\mathcal{C}_{\bar{k}}$ lying on both Γ_1 and Γ_2 (in particular, Y_C may have loops and multiple edges). We view Y_C as a metric space where we give each edge length 1. Denote by $H_1(Y_C, \mathbb{Z})$ the first singular homology group of Y_C. Since $\mathcal{C}_{\bar{k}}$ is the base change

from k to $\bar{k}$ of the special fibre of C, $H_1(Y_C, \mathbb{Z})$ carries a natural G_k-action.[†] Moreover, $H_1(Y_C, \mathbb{Z})$ carries a natural non-degenerate, symmetric, G_k-invariant bilinear pairing

$$P : H_1(Y_C, \mathbb{Z}) \times H_1(Y_C, \mathbb{Z}) \to \mathbb{Z}$$

(informally, $P(\gamma, \gamma')$ is the signed length of $\gamma \cap \gamma'$). The pairing P induces an injection

$$H_1(Y_C, \mathbb{Z}) \hookrightarrow H_1(Y_C, \mathbb{Z})^\vee := \mathrm{Hom}(H_1(Y_C, \mathbb{Z}), \mathbb{Z}), \tag{11.3}$$

sending γ to $P(-, \gamma)$. The component group $\Phi(\bar{k})$ of J/K is then G_k-equivariantly isomorphic to the cokernel of this map:

$$\Phi(\bar{k}) = H_1(Y_C, \mathbb{Z})^\vee / H_1(Y_C, \mathbb{Z}). \tag{11.4}$$

In particular, we have

$$c(J/K) = \left| \left(\frac{H_1(Y_C, \mathbb{Z})^\vee}{H_1(Y_C, \mathbb{Z})} \right)^{G_k} \right|. \tag{11.5}$$

Moreover, the root number $w(J/K)$ of J is encoded in the G_k-invariants of $H_1(Y_C, \mathbb{Z})$:

$$w(J/K) = (-1)^{\mathrm{rk} H_1(Y_C, \mathbb{Z})^{G_k}}.$$

If we replace K by L and repeat the above constructions for the base change C_L of C to L, then the dual graph Y_{C_L} is obtained from Y_C by replacing each edge by a path consisting of two edges.[‡] In particular, the homology of the new dual graph with its G_k-action is unchanged, but the pairing gets multiplied by 2. Thus, we have

$$c(J/L) = \left| \left(\frac{H_1(Y_C, \mathbb{Z})^\vee}{2 H_1(Y_C, \mathbb{Z})} \right)^{G_k} \right| \quad \text{and} \quad w(J/L) = (-1)^{\mathrm{rk} H_1(Y_C, \mathbb{Z})^{G_k}}. \tag{11.6}$$

11.2 | The group $\mathfrak{B}_{C/K}$

Following work of Betts–Dokchitser [4], the quantities appearing in (11.5) and (11.6) can be neatly packaged together in the following way. Temporarily writing $\Lambda = H^1(Y_C, \mathbb{Z})$, define the finite

---

[†] Due to the possible presence of loops and multiple edges in Y_C, the G_k-action on $H_1(Y_C, \mathbb{Z})$ need not be fully determined by the G_k-action on the irreducible components of $C_{\bar{k}}$. When there is ambiguity, one needs some additional information concerning the ordinary double points to pin down the action; see, for example, [18, Section 2.1] for more details.

[‡] To see this, one can argue as follows. Firstly, the base change of C to the ring of integers $\mathcal{O}_{K^{nr}}$ coincides with the minimal regular model $C'/\mathcal{O}_{K^{nr}}$ of C over $\mathcal{O}_{K^{nr}}$; hence, $C_{\bar{k}}$ coincides with the special fibre of C'. Since C' is both semistable and regular, each singular point x of $C_{\bar{k}}$ is a split ordinary double point of thickness 1 (in the sense of [29, Definition 10.3.23]). After base-changing C' to $\mathcal{O}_{L^{nr}}$, the point x becomes an ordinary double point of thickness 2 in $C' \times_{\mathcal{O}_{K^{nr}}} \mathcal{O}_{L^{nr}}$, as follows from the description of the completed local ring at x given in [29, Corollary 3.22] (the factor 2 arising as the ramification index of L/K). The minimal regular model of C_L over $\mathcal{O}_{L^{nr}}$ is then obtained by blowing up $C' \times_{\mathcal{O}_{K^{nr}}} \mathcal{O}_{L^{nr}}$ once at each such x, which has the claimed effect on the dual graph (cf. [29, Lemma 10.3.21, Corollary 10.3.25]).

abelian group $\mathfrak{B}_{C/K}$ by

$$\mathfrak{B}_{C/K} = \mathrm{im}\bigl(H^1(G_k, \Lambda) \longrightarrow H^1(G_k, \Lambda^\vee)\bigr), \tag{11.7}$$

where the map is induced by (11.3). Combining (11.5) and (11.6) with [4, Theorem 1.4.2] then gives

$$w(J/L) \cdot (-1)^{\mathrm{ord}_2 \frac{c(J/L)}{c(J/K)}} = (-1)^{\dim \mathfrak{B}_{C/K}[2]}. \tag{11.8}$$

Remark 11.9. If $\mathcal{T}$ denotes the toric part of the Raynaud parametrisation of J/K, and $X(\mathcal{T})$ denotes its character group, then $X(\mathcal{T})$ carries a natural G_k-action and a non-degenerate symmetric pairing $X(\mathcal{T}) \otimes X(\mathcal{T}) \to \mathbb{Z}$ (see [23, 52]). As explained in [18, Section 2], it follows from work of Raynaud that $X(\mathcal{T}) \cong H_1(G_k, \mathbb{Z})$ as G_k-modules with a pairing. One can then alternatively obtain (11.8) directly from [4, Theorem 1.1.1 (i)].

11.3 | Strategy for the proof of Proposition 11.1

In light of (11.2) and (11.8), Conjecture 1.7 for C and L/K is the equivalent to the assertion

$$(-1)^{\dim \mathfrak{B}_{C/K}[2]} \overset{?}{=} (-1)^{\mathrm{ord}_2 c(J^L/K)} (\Delta_C, L/K)(-1)^{\epsilon(C/K) + \epsilon(C^L/K)}. \tag{11.10}$$

In Section 12 below, we give a general result, Proposition 12.18, which facilitates the computation of the parity of the dimension of the 2-torsion of the group

$$\mathfrak{B}_\Lambda := \mathrm{im}\bigl(H^1(G_k, \Lambda) \longrightarrow H^1(G_k, \Lambda^\vee)\bigr)$$

associated to an arbitrary G_k-lattice Λ equipped with a non-degenerate symmetric bilinear pairing.

In Section 13, we summarise results from [18] which give an explicit description of the lattice $H_1(Y_C, \mathbb{Z})$ attached to a semistable hyperelliptic curve $C/K : y^2 = f(x)$ in terms of combinatorial data associated to the p-adic distances between the roots of $f(x)$. Combined with the results of Section 12 mentioned above, this enables the explicit computation of $\dim \mathfrak{B}_{C/K}[2]$ (mod 2) for arbitrary semistable hyperelliptic curves; we present the result of this computation as Corollary 13.25. (Strictly speaking, we only carry out these computations over a suitably large odd degree unramified extension of K. This suffices for the application to Conjecture 1.7 thanks to Lemma 4.1, and has the advantage that several statements in [18] simplify after such an extension.)

Separately, in Section 14, we present an explicit combinatorial description of the minimal proper regular model of a ramified quadratic twist of a semistable hyperelliptic curve. This will be deduced from work of Faraggi–Nowell [20] which more generally describes the minimal regular strict normal crossings (SNC) model of a hyperelliptic curve X over a local field of odd residue characteristic, under the assumption that X attains semistable reduction after a tamely ramified extension of the base field. We combine this description with Proposition 10.8 to describe explicitly the quantity $(-1)^{\mathrm{ord}_2 c(J^L/K) + \epsilon(C^L/K)}$; we present this result as Corollary 14.31.

Finally, in Section 15, we combine Corollaries 13.25 and 14.31 to establish (11.10).

12 │ THE PARITY OF dim $\mathfrak{B}_\Lambda[2]$

The aim of this section is to prove Proposition 12.18, which gives an explicit criterion for determining the parity of dim $\mathfrak{B}_\Lambda[2]$, where $\mathfrak{B}_\Lambda$ is the group defined in Section 12.1 below and considered by Betts–Dokchitser in [4]. This can be viewed as a complement to the results of [4, Section 2].

Let k be a finite field. Take Λ to be a (discrete) $\mathbb{Z}[G_k]$-module, free and of finite rank as a $\mathbb{Z}$-module, and equipped with a non-degenerate G_k-invariant symmetric bilinear pairing

$$\langle \, , \, \rangle : \Lambda \times \Lambda \longrightarrow \mathbb{Z}. \tag{12.1}$$

We extend $\langle \, , \, \rangle$ bilinearly to a pairing on the $\mathbb{Q}[G_k]$-module $V := \Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ and write $\Lambda^\vee$ for the dual lattice

$$\Lambda^\vee = \{v \in V \ : \ \langle v, \lambda \rangle \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\}. \tag{12.2}$$

The map $v \mapsto \langle v, - \rangle$ identifies $\Lambda^\vee$ with $\mathrm{Hom}(\Lambda, \mathbb{Z})$. We denote by Φ the finite abelian group $\Lambda^\vee/\Lambda$, the discriminant group of the lattice. The pairing on V restricts to a G_k-invariant pairing $\Lambda^\vee \times \Lambda \to \mathbb{Z}$, and further induces a non-degenerate symmetric bilinear pairing

$$\overline{\langle \, , \, \rangle} : \Phi \times \Phi \longrightarrow \mathbb{Q}/\mathbb{Z}. \tag{12.3}$$

12.1 │ The group $\mathfrak{B}_\Lambda$

Define the finite abelian group

$$\mathfrak{B}_\Lambda := \mathrm{im}\big(H^1(G_k, \Lambda) \longrightarrow H^1(G_k, \Lambda^\vee)\big) = \ker\big(H^1(G_k, \Lambda^\vee) \longrightarrow H^1(G_k, \Phi)\big).$$

Consider the pairing

$$H^1(G_k, \Lambda) \otimes H^1(G_k, \Lambda) \longrightarrow H^2(G_k, \mathbb{Z}) \xrightarrow{\sim} H^1(G_k, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\text{eval. at } F} \mathbb{Q}/\mathbb{Z}. \tag{12.4}$$

Here, the first map is composition of cup-product with the pairing (12.1), and the second is the inverse of the coboundary map $\delta : H^1(G_k, \mathbb{Q}/\mathbb{Z}) \to H^2(G_k, \mathbb{Z})$ arising from the short exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \tag{12.5}$$

The final map is given by evaluating cocycles at the Frobenius element $F \in G_k$.

We have the following result of Betts–Dokchitser.

Proposition 12.6. *Lifting to $H^1(G_k, \Lambda)$ and applying the pairing (12.4) induces a non-degenerate antisymmetric bilinear pairing*

$$(\, , \,) : \mathfrak{B}_\Lambda \times \mathfrak{B}_\Lambda \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Proof. This is [4, Proposition 2.2.2]. The key point is the anti-symmetry of the top pairing, and non-degeneracy of the bottom pairing, in the commutative diagram

$$
\begin{array}{ccc}
H^1(G_k, \Lambda) \otimes H^1(G_k, \Lambda) & \xrightarrow{\ \cup\ } & H^2(G_k, \mathbb{Z}) \\
\downarrow{\scriptstyle \alpha \otimes 1} & & \| \\
H^1(G_k, \Lambda^\vee) \otimes H^1(G_k, \Lambda) & \xrightarrow{\ \cup\ } & H^2(G_k, \mathbb{Z}),
\end{array}
\tag{12.7}
$$

where α is induced by the inclusion of Λ into $\Lambda^\vee$. See [4, Proposition 2.2.2] for a proof of these facts. $\qquad\square$

Corollary 12.8. *The order of $\mathfrak{B}_\Lambda$ is either a square or twice a square. Moreover, $\mathfrak{B}_\Lambda$ has square order if and only if* $\dim \mathfrak{B}_\Lambda[2]$ *is even.*

Proof. This is a formal consequence of the existence of a non-degenerate antisymmetric $\mathbb{Q}/\mathbb{Z}$-valued bilinear pairing on $\mathfrak{B}_\Lambda$; see [4, Theorem 2.4.1] for a proof. $\qquad\square$

Now consider the map $\mathfrak{B}_\Lambda \to \mathbb{Q}/\mathbb{Z}$ given by $x \mapsto (x, x)$. This is a homomorphism by antisymmetry of $(\ ,\ )$, so by non-degeneracy, there is a unique $\mathfrak{c} \in \mathfrak{B}_\Lambda$ such that

$$
(x, x) = (\mathfrak{c}, x) \quad \text{for all } x \in \mathfrak{B}_\Lambda.
\tag{12.9}
$$

It follows from the arguments of [51, Section 6] that one has

$$
\dim \mathfrak{B}_\Lambda[2] \equiv 0 \pmod 2 \quad \text{if and only if} \quad (\mathfrak{c}, \mathfrak{c}) = 0.
\tag{12.10}
$$

In Lemma 12.15 below, we give an explicit description of this class $\mathfrak{c}$. The construction involves quadratic refinements of the pairings (12.1) and (12.3).

12.2 | Quadratic refinements of the pairings (12.1) and (12.3)

We begin with some notation.

Notation 12.11. For abelian groups A and M, call a function $q : A \to M$ a quadratic map if the function $B_q : A \times A \to M$ defined by $B_q(a_1, a_2) = q(a_1 + a_2) - q(a_1) - q(a_2)$ is bilinear. We call q a quadratic form if, moreover, for all $a \in A$ and $n \in \mathbb{Z}$, we have $q(na) = n^2 q(a)$. We say that q is a quadratic refinement of B_q. Denote by $\mathcal{Q}_\Lambda$ the set of $\mathbb{Z}$-valued quadratic refinements of (12.1), and by $\mathcal{Q}_\Phi$, the set of $\mathbb{Q}/\mathbb{Z}$-valued quadratic refinements of (12.3).

Now define the subset $S \subseteq V$ as

$$
S = \left\{ v \in \Lambda^\vee \ : \ \langle \lambda, \lambda \rangle \equiv \langle \lambda, v \rangle \pmod 2 \ \text{ for all } \lambda \in \Lambda \right\}.
\tag{12.12}
$$

One checks using the fact that $\lambda \mapsto \langle \lambda, \lambda \rangle$ (mod 2) is a homomorphism that S is non-empty. For $v \in S$, denote by $q_v : \Lambda \to \mathbb{Z}$ the quadratic map

$$q_v(\lambda) = \tfrac{1}{2}(\langle \lambda, \lambda \rangle + \langle \lambda, v \rangle). \tag{12.13}$$

Sending v to q_v gives a bijection from S to $\mathcal{Q}_\Lambda$. Moreover, taking $\lambda \in \Lambda^\vee$ in the formula (12.13), and then reducing modulo $\mathbb{Z}$, gives a quadratic refinement $\overline{q}_v : \Phi \to \mathbb{Q}/\mathbb{Z}$ of the pairing (12.3). This is a quadratic form if and only if $v \in \Lambda$. The map $v \mapsto \overline{q}_v$ is a bijection between $S/2\Lambda$ (the quotient of S by the action of 2Λ) and $\mathcal{Q}_\Phi$.

12.3 | Cohomology classes associated to quadratic refinements

Since the pairing (12.1) is G_k-invariant, G_k acts on $\mathcal{Q}_\Lambda$. Explicitly, for $\sigma \in G_k$ and $q \in \mathcal{Q}_\Lambda$, we define $^\sigma q : \Lambda \to \mathbb{Z}$ by setting $^\sigma q(\lambda) = q(\sigma^{-1}\lambda)$. Given $q_1, q_2 \in \Lambda$, we have $q_1 - q_2 \in \mathrm{Hom}(\Lambda, \mathbb{Z}) = \Lambda^\vee$; thus, $\Lambda^\vee$ acts simply transitively on $\mathcal{Q}_\Lambda$. In particular, associated to $\mathcal{Q}_\Lambda$ is a class $\mathbf{q}_\Lambda \in H^1(G_k, \Lambda^\vee)$, explicitly represented by the 1-cocycle $\sigma \mapsto {}^\sigma q - q$ for any $q \in \mathcal{Q}_\Lambda$. We similarly have $\mathbf{q}_\Phi \in H^1(G_k, \Phi)$ associated to $\mathcal{Q}_\Phi$.[†]

Remark 12.14. The discussion in Section 12.2 above provides a more explicit description of the classes $\mathbf{q}_\Lambda$ and $\mathbf{q}_\Phi$. Let $v \in S$ and let q_v (resp. $\overline{q}_v$) be the associated element of $\mathcal{Q}_\Lambda$ (resp. $\mathcal{Q}_\Phi$). Computing the associated cocycles, one sees that $\mathbf{q}_\Lambda$ and $\mathbf{q}_\Phi$ are represented by the 1-cocycles

$$\sigma \mapsto \tfrac{1}{2}(\sigma v - v) \in \Lambda^\vee \quad \text{and} \quad \sigma \mapsto \tfrac{1}{2}(\sigma v - v) \pmod{\Lambda},$$

respectively. Note, in particular, that $\mathbf{q}_\Lambda$ maps to $\mathbf{q}_\Phi$ under the natural map $H^1(G_k, \Lambda^\vee) \to H^1(G_k, \Phi)$.

Lemma 12.15. *With the notation above, we have the following.*

(i) *The element $\mathbf{q}_\Lambda \in H^1(G_k, \Lambda^\vee)$ lies in $\mathfrak{B}_\Lambda$.*
(ii) *We have $(x, x) = (\mathbf{q}_\Lambda, x)$ for all $x \in \mathfrak{B}_\Lambda$. Thus, $\mathbf{q}_\Lambda$ is the class $\mathfrak{c}$ of Section 12.1.*

Proof. It follows from [48, Corollary 2.8] that for all $\rho \in H^1(G_k, \Lambda)$, we have

$$\mathbf{q}_\Lambda \cup \rho = \rho \cup \rho \quad \text{inside } H^2(G_k, \mathbb{Z}). \tag{12.16}$$

Here, both cup-products are induced by the pairing $\langle \, , \, \rangle$. From this identity and commutativity of (12.7), it follows that $\mathbf{q}_\Lambda \cup \rho = 0$ for all $\rho \in \ker(H^1(G_k, \Lambda) \to H^1(G_k, \Lambda^\vee))$. It now follows formally from the stated properties of the pairings in (12.7) that $\mathbf{q}_\Lambda \in \mathfrak{B}_\Lambda$. This proves part (i), and part (ii) now follows from (12.16) and the definition of the pairing $(\, , \,)$ on $\mathfrak{B}_\Lambda$. □

Remark 12.17. Since $\mathbf{q}_\Lambda$ is a lift of $\mathbf{q}_\Phi$ to $H^1(G_k, \Lambda^\vee)$, it follows from Lemma 12.15 (i) that the class $\mathbf{q}_\Phi \in H^1(G_k, \Phi)$ is trivial. In particular, the pairing (12.3) on Φ admits a G_k-invariant quadratic

---

[†] To be more precise, mimicking the construction of $\mathbf{q}_\Lambda$ yields a class in $H^1(G_k, \Phi^*)$ where $\Phi^* = \mathrm{Hom}(\Phi, \mathbb{Q}/\mathbb{Z})$; we transport this class to $H^1(G_k, \Phi)$ via the isomorphism $\Phi \xrightarrow{\sim} \Phi^*$ provided by the pairing (12.3).

refinement. From the discussion in Section 12.2, such a quadratic refinement is necessarily of the form $\overline{q}_v$ for some $v \in S$. The G_k-invariance of $\overline{q}_v$ means that such a v satisfies $\sigma v - v \in 2\Lambda$ for all $\sigma \in G_k$.

12.4 | The order of $\mathfrak{B}_\Lambda$ modulo squares

We now give the promised criterion for determining the parity of $\dim \mathfrak{B}_\Lambda[2]$. As usual, $F \in G_k$ denotes the Frobenius element. The set S is as defined in (12.12).

Proposition 12.18. *There exists $x \in S$ such that $\frac{1}{2}(Fx - x) \in \Lambda$. For any such x, we have*

$$\dim \mathfrak{B}_\Lambda[2] \equiv \left\langle x, \tfrac{1}{2}(Fx - x) \right\rangle \ (mod\ 2).$$

Proof. For existence, take any $x \in S$ for which the associated quadratic form $\overline{q}_x$ is G_k-invariant (cf. Remark 12.17).

Now fix such an x and denote by $a : G_k \to \Lambda$ the 1-cocycle $a(\sigma) = \frac{1}{2}(\sigma x - x)$. Its class in $H^1(G_k, \Lambda)$ is a lift of $\mathfrak{q}_\Lambda \in \mathfrak{B}_\Lambda$ to $H^1(G_k, \Lambda)$. Consider the commutative diagram

$$\begin{array}{ccc}
H^0(G_k, V/\Lambda^\vee) \otimes H^1(G_k, \Lambda) & \xrightarrow{\ \cup\ } & H^1(G_k, \mathbb{Q}/\mathbb{Z}) \\
\Big\downarrow{\scriptstyle \delta \otimes 1} & & \Big\downarrow{\scriptstyle \delta} \\
H^1(G_k, \Lambda^\vee) \otimes H^1(G_k, \Lambda) & \xrightarrow{\ \cup\ } & H^2(G_k, \mathbb{Z}).
\end{array} \qquad (12.19)$$

Here, the coboundary maps δ arise from the short exact sequence (12.5) and the corresponding sequence given by tensoring (12.5) by $\Lambda^\vee$, and both cup-products are induced by the pairing $\langle\,,\,\rangle$. The element $\frac{1}{2}x \in V/\Lambda^\vee$ defines an element of $H^0(G_k, V/\Lambda^\vee)$ which maps under δ to $\mathfrak{q}_\Lambda$. From commutativity of (12.19) and the definition of the pairing $(\,,\,)$ on $\mathfrak{B}_\Lambda$, we find

$$(\mathfrak{q}_\Lambda, \mathfrak{q}_\Lambda) = \left\langle \tfrac{1}{2}x, a(F) \right\rangle = \tfrac{1}{2}\left\langle x, \tfrac{1}{2}(Fx - x) \right\rangle \in \tfrac{1}{2}\mathbb{Z}/\mathbb{Z}.$$

The result now follows from (12.10) and Lemma 12.15 (ii). $\qquad\square$

Remark 12.20. Identifying $\Lambda^\vee$ with $\mathrm{Hom}(\Lambda, \mathbb{Z})$ via the map $v \mapsto \langle v, - \rangle$ leads to the following rephrasing of Proposition 12.18: given $\phi \in \mathrm{Hom}(\Lambda, \mathbb{Z})$ such that $\langle \lambda, \lambda \rangle \equiv \phi(\lambda) \pmod 2$ for all $\lambda \in \Lambda$, and such that $\frac{1}{2}(F\phi - \phi) = \langle \lambda, - \rangle$ for a (necessarily unique) $\lambda \in \Lambda$, we have

$$\dim \mathfrak{B}_\Lambda[2] \equiv \phi(\lambda) \pmod 2.$$

Indeed, the unique $x \in \Lambda^\vee$ for which $\phi = \langle x, - \rangle$ satisfies the conditions of Proposition 12.18.

13 | CLUSTERS AND THE GROUP $\mathfrak{B}_{C/K}$ FOR SEMISTABLE HYPERELLIPTIC CURVES

We take the notation of Section 11. In particular, K denotes a non-archimedean local field with residue field k of odd characteristic, and C/K denotes a hyperelliptic curve with semistable reduction. We henceforth fix a Weierstrass equation $y^2 = f(x)$ for C, where $f(x) \in K[x]$ is a squarefree polynomial of degree $2g + 1$ or $2g + 2$ for $g \geqslant 2$ the genus of C. We denote by $\mathcal{R}$ the set of roots of $f(x)$ in K^s and denote by c_f the leading coefficient of $f(x)$. Thus,

$$f(x) = c_f \prod_{r \in \mathcal{R}} (x - r).$$

13.1 | Clusters

We now recall several results from [18], which provide a framework for studying invariants of hyperelliptic curves over local fields of odd residue characteristic. We refer to that work for more details (cf. also [2]). The central object is that of a *cluster*. In what follows we denote by $v : \bar{K} \to \mathbb{Q} \cup \{\infty\}$ the extension to $\bar{K}$ of the normalised valuation on K.

Definition 13.1. A *cluster* is a non-empty subset $\mathfrak{s} \subset \mathcal{R}$ of the form $\mathfrak{s} = D \cap \mathcal{R}$ for some disc $D = \{x \in \bar{K} \mid v(x - z) \geqslant d\}$ where $z \in \bar{K}$ and $d \in \mathbb{Q}$. If $|\mathfrak{s}| > 1$, then $\mathfrak{s}$ is said to be *proper* and its *depth* $d_{\mathfrak{s}}$ is defined as

$$d_{\mathfrak{s}} = \min_{r, r' \in \mathfrak{s}} v(r - r').$$

We call any element $z_{\mathfrak{s}}$ of the minimal disc cutting out a proper cluster $\mathfrak{s}$ a *centre* for $\mathfrak{s}$.

We summarise some terminology for clusters.

Definition 13.2. Given clusters $\mathfrak{s}_1 \neq \mathfrak{s}_2$ with $\mathfrak{s}_1$ a maximal subcluster of $\mathfrak{s}_2$, we say that $\mathfrak{s}_1$ is a *child* of $\mathfrak{s}_2$, denote this $\mathfrak{s}_1 < \mathfrak{s}_2$, and refer to $\mathfrak{s}_2$ as the *parent* of $\mathfrak{s}_1$. Any cluster $\mathfrak{s} \neq \mathcal{R}$ has a unique parent $P(\mathfrak{s})$. We define the *relative depth* of a proper cluster $\mathfrak{s} \neq \mathcal{R}$ as

$$\delta_{\mathfrak{s}} := d_{\mathfrak{s}} - d_{P(\mathfrak{s})} \geqslant 0.$$

We call a cluster *even* (resp. *odd*) if it contains an even (resp. odd) number of roots, and call it *übereven* if it is even and all its children are even also. We call a cluster $\mathfrak{s}$ *principal* if $|\mathfrak{s}| \geqslant 3$, save when either $\mathfrak{s} = \mathcal{R}$ is even and has exactly two children, or when $\mathfrak{s}$ has a child of size $2g$. A cluster of size 2 is called a *twin*, and a non-übereven cluster that has a child of size $2g$ is called a *cotwin*. For a principal cluster $\mathfrak{s}$ which is not übereven, its *genus* $g(\mathfrak{s})$ is defined as

$$g(\mathfrak{s}) = \left\lfloor \frac{1}{2}(\#\{\text{odd children of } \mathfrak{s}\} - 1) \right\rfloor.$$

We define the genus of an übereven cluster to be 0. Finally, for clusters $\mathfrak{s}_1, \mathfrak{s}_2$, we write $\mathfrak{s}_1 \wedge \mathfrak{s}_2$ for the smallest cluster containing both $\mathfrak{s}_1$ and $\mathfrak{s}_2$.
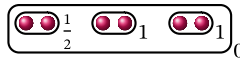
Example 13.3. Take C to be the hyperelliptic curve

$$C/\mathbb{Q}_3 : y^2 = (x^2 + 3)((x - i)^2 - 3^2)((x + i)^2 - 3^2)$$

considered in Example 9.12, where i is a square root of -1. The proper clusters are

$$\mathcal{R} = \{ \pm i\sqrt{3}, i \pm 3, -i \pm 3 \}, \ \mathfrak{t}_1 = \{ \pm i\sqrt{3} \}, \ \mathfrak{t}_2 = \{ i \pm 3 \}, \ \mathfrak{t}_3 = \{ -i \pm 3 \}.$$

The unique principal cluster is $\mathcal{R}$ and it is übereven, has depth 0 and genus 0. There are three twins: $\mathfrak{t}_1$, $\mathfrak{t}_2$ and $\mathfrak{t}_3$, and we have $\delta_{\mathfrak{t}_1} = 1/2$, $\delta_{\mathfrak{t}_2} = \delta_{\mathfrak{t}_3} = 1$. We display this information pictorially as shown:

$$\boxed{\ \overset{\bullet\,\bullet}{}{}_{\frac{1}{2}} \ \overset{\bullet\,\bullet}{}{}_{1} \ \overset{\bullet\,\bullet}{}{}_{1}\ }_{0}$$

Here we draw roots as $\bullet$ and draw ovals around roots to represent a proper cluster. The subscript on the outer cluster is its depth, and on all other clusters, it is the relative depth. We refer to this diagram as the *cluster picture* of C.

We remark that the description of the minimal regular model of C given previously in Example 9.12 now follows immediately from [18, Theorems 1.11 and 8.6].

For the rest of this section, we make the following assumption, which will lead to several simplifications in the results of [18].

Assumption 13.4. We assume that $|\mathcal{R}| = 2g + 2$ and that there are no clusters of size $2g$ or $2g + 1$.

Remark 13.5. By [18, Theorem 15.2], any semistable hyperelliptic curve over K is isomorphic to a curve satisfying Assumption 13.4 over any suitably large odd degree unramified extension of K (the key point being that if the residue field of K is sufficiently large, then one can make a change of variables to force Assumption 13.4 to be satisfied).

We now summarise certain results from [18], using Assumption 13.4 to simplify several statements. Firstly, the fact that C is semistable forces several constraints on the possible clusters and their depths. Specifically, we have the following.

Theorem 13.6 [18] Theorem 1.8. *Semistability of C is equivalent to the following three conditions:*

(1) *the extension $K(\mathcal{R})/K$ has ramification degree at most 2,*
(2) *every proper cluster is invariant under the action of the inertia group of K,*
(3) *every principal cluster $\mathfrak{s}$ has $d_\mathfrak{s} \in \mathbb{Z}$ and $\nu_\mathfrak{s} \in 2\mathbb{Z}$,*

where $\nu_\mathfrak{s}$ is the quantity

$$\nu_\mathfrak{s} = v(c_f) + |\mathfrak{s}|d_\mathfrak{s} + \sum_{r \notin \mathfrak{s}} d_{\{r\} \wedge \mathfrak{s}}. \tag{13.7}$$

Note that by part (1) of Theorem 13.6, each inertia orbit of roots has size at most 2 (i.e. the irreducible factors of $f(x)$ over K^{nr} are linear or quadratic), and every cluster $\mathfrak{s}$ has $d_{\mathfrak{s}} \in \frac{1}{2}\mathbb{Z}$. The set of proper clusters $\mathfrak{s}$ with $d_{\mathfrak{s}} \notin \mathbb{Z}$ will be of particular importance.

Notation 13.8. Let T denote the set of proper clusters $\mathfrak{s}$ with $d_{\mathfrak{s}} \notin \mathbb{Z}$.

Lemma 13.9. *If $r \neq r'$ are inertia conjugate elements of $\mathcal{R}$, then $\mathfrak{s} = \{r, r'\}$ is a cluster with $d_{\mathfrak{s}} \notin \mathbb{Z}$. Moreover, every proper cluster $\mathfrak{s}$ with $d_{\mathfrak{s}} \notin \mathbb{Z}$ takes this form.*

Proof. If r and r' are inertia conjugate roots, then $v(r - r') \in 1/2 + \mathbb{Z}$ (cf. [18, Lemma C.2]), so the minimal cluster containing both r and r' has non-integer depth. In light of Assumption 13.4, it follows from [18, Lemma 4.2] that $\{r, r'\}$ is a cluster. Moreover, [18, Lemma 4.2] shows further that any proper cluster $\mathfrak{s}$ with $d_{\mathfrak{s}} \notin \mathbb{Z}$ takes this form. □

A consequence of Lemma 13.9 is that T is naturally in bijection with the set of inertia-conjugate pairs of roots of $f(x)$.

13.2 | Signs associated to clusters

By Theorem 13.6(2), the assumption that C is semistable means that $\mathrm{Gal}(K^{\mathrm{nr}}/K) = G_k$ acts on the set of proper clusters. We will augment this action by adding in certain signs associated to even clusters (cf. [18, Definition 1.12]).

Notation 13.10. For a cluster $\mathfrak{s}$, we write $\mathfrak{s}^*$ for the smallest cluster $\mathfrak{s}^* \supseteq \mathfrak{s}$ whose parent is not übereven, and set $\mathfrak{s}^* = \mathcal{R}$ if no such cluster exists.

Definition 13.11. For even clusters $\mathfrak{s}$, fix a choice of $\theta_{\mathfrak{s}} = \sqrt{c_f \prod_{r \notin \mathfrak{s}}(z_{\mathfrak{s}} - r)}$, where z_s is any centre for $\mathfrak{s}$. Still assuming $\mathfrak{s}$ is even, define $\epsilon_{\mathfrak{s}} : G_K \to \{\pm 1\}$ by

$$\epsilon_{\mathfrak{s}}(\sigma) \equiv \frac{\sigma(\theta_{\mathfrak{s}^*})}{\theta_{(\sigma \mathfrak{s})^*}} \mod \mathfrak{m}.$$

Here, $\mathfrak{m}$ denotes the maximal ideal of the ring of integers of $\bar{K}$, so that 'mod $\mathfrak{m}$' denotes reduction to the residue field $\bar{k}$.

Remark 13.12. If $\mathfrak{s} \neq \mathcal{R}$ is an even cluster, or $\mathfrak{s} = \mathcal{R}$ is übereven, then

$$v\left(c_f \prod_{r \notin \mathfrak{s}}(z_{\mathfrak{s}} - r)\right) = \nu_{\mathfrak{s}} - |\mathfrak{s}|d_{\mathfrak{s}}$$

is an even integer (here $\nu_{\mathfrak{s}}$ is as defined in the statement of Theorem 13.6). Indeed, by [18, Lemma C.5], we have $\nu_{\mathfrak{s}} - |\mathfrak{s}|d_{\mathfrak{s}} = \nu_{P(\mathfrak{s})} - |\mathfrak{s}|d_{P(\mathfrak{s})}$, and by Lemmas 4.2 and 4.9 of op. cit., we see that one of $\mathfrak{s}$ or $P(\mathfrak{s})$ must have both integral depth and even ν. In particular, it follows that $\theta_{\mathfrak{s}} \in K^{\mathrm{nr}}$. Thus, $\epsilon_{\mathfrak{s}}$ descends to a function $G_k \to \{\pm 1\}$.

Remark 13.13. As explained in [18, Remark 1.14], although the function $\epsilon_\mathfrak{s}$ depends on the choice of $\theta_\mathfrak{s}$, the restriction of $\epsilon_\mathfrak{s}$ to the stabiliser of $\mathfrak{s}$ does not. In fact, if $K_\mathfrak{s}$ denotes the fixed field of $\bar{K}$ by the stabiliser of $\mathfrak{s}$, then $K_\mathfrak{s}$ is a finite unramified extension of K, $\theta_{\mathfrak{s}^*}^2 \in K_\mathfrak{s}$, and $\epsilon_\mathfrak{s}$ restricted to the stabiliser of $\mathfrak{s}$ is the quadratic character associated to the extension $K_\mathfrak{s}(\theta_{\mathfrak{s}^*})/K_\mathfrak{s}$.

Example 13.14. Let C be as in Example 13.3 and let $\mathfrak{s}$ be any of the four even clusters. Then, we have $\mathfrak{s}^* = \mathcal{R}$. We can take $z_\mathcal{R} = 0$ and $\theta_\mathcal{R} = 1$. Then $\epsilon_\mathfrak{s}(\sigma) = 1$ for all σ.

We remark that the description of the Frobenius action on the special fibre of the minimal regular model of C detailed previously in Example 9.12 can be read off from this data, coupled with the Frobenius action on the set of proper clusters; see [18, Theorems 8.6].

13.3 | Description of the lattice

We retain the notation from Section 11.1. In particular, Y_C denotes the dual graph of the (geometric special fibre of the) minimal proper regular model of C. Here, we recall from [18] a description of the $\mathbb{Z}[G_k]$-module $H_1(Y_C, \mathbb{Z})$ along with its associated pairing. It will be convenient to first define an auxiliary lattice Π which is closely related to $H_1(Y_C, \mathbb{Z})$, but which is simpler to describe.

Definition 13.15. Let A be the set of even non-übereven clusters excluding $\mathcal{R}$, and define Π to be the free $\mathbb{Z}$-module with basis $\{\ell_\mathfrak{s} : \mathfrak{s} \in A\}$, so that

$$\Pi = \bigoplus_{\mathfrak{s} \in A} \mathbb{Z}\ell_\mathfrak{s}.$$

Further, let B be the subset of A consisting of clusters $\mathfrak{s}$ with $\mathfrak{s}^* = \mathcal{R}$. We endow Π with the symmetric pairing

$$\langle \, , \, \rangle : \Pi \times \Pi \longrightarrow \mathbb{Z}$$

given by

$$\langle \ell_{\mathfrak{s}_1}, \ell_{\mathfrak{s}_2} \rangle = \begin{cases} 0 & \mathfrak{s}_1^* \neq \mathfrak{s}_2^*, \\ 2\big(d_{\mathfrak{s}_1 \wedge \mathfrak{s}_2} - d_{P(\mathfrak{s}_1^*)}\big) & \mathfrak{s}_1, \mathfrak{s}_2 \notin B, \ \ \mathfrak{s}_1^* = \mathfrak{s}_2^*, \\ 2\big(d_{\mathfrak{s}_1 \wedge \mathfrak{s}_2} - d_\mathcal{R}\big) & \mathfrak{s}_1, \mathfrak{s}_2 \in B. \end{cases} \qquad (13.16)$$

We further endow Π with the G_k-action given by $\sigma \cdot \ell_\mathfrak{s} = \epsilon_\mathfrak{s}(\sigma)\ell_{\sigma\mathfrak{s}}$. Note that the pairing $\langle \, , \, \rangle$ is invariant for this action.

It will be useful to note that the pairing on $\Pi/2\Pi$ induced from that on Π has a very simple form.

Lemma 13.17. *For all clusters $\mathfrak{s}_1, \mathfrak{s}_2 \in A$, we have*

$$\big\langle \ell_{\mathfrak{s}_1}, \ell_{\mathfrak{s}_2} \big\rangle \equiv \begin{cases} 1 \pmod 2 & \mathfrak{s}_1 = \mathfrak{s}_2 \in T, \\ 0 \pmod 2 & \text{else.} \end{cases}$$

Proof. Combine Lemma 13.9 with the formula (13.16). □

Definition 13.18. Define the lattice

$$\Lambda = \left\{ \sum_{\mathfrak{s} \in A} a_{\mathfrak{s}} \ell_{\mathfrak{s}} \in \Pi \ \Big| \ \sum_{\mathfrak{s} \in B} a_{\mathfrak{s}} = 0 \right\}$$

along with the pairing and G_k-action induced from that on Π.

Theorem 13.19 [18] Theorem 1.14. *We have* $\Lambda \cong H_1(Y_C, \mathbb{Z})$ *as* $\mathbb{Z}[G_k]$-*modules equipped with a pairing.*

13.4 | The group $\mathfrak{B}_{C/K}$ for semistable hyperelliptic curves

Let $\mathfrak{B}_{C/K}$ be the group defined in (11.7). Let Λ be as in Definition 13.18 above, and let $\mathfrak{B}_\Lambda$ be the associated group defined in Section 12.1. By Theorem 13.19, we have $\mathfrak{B}_{C/K} \cong \mathfrak{B}_\Lambda$. Recall from Notation 13.8 the definition of the set T. We denote by $F \in G_k$ the Frobenius element, and for a cluster $\mathfrak{s}$, we denote by $\mathrm{Orb}_{\mathfrak{s}}$ its G_k-orbit.

Proposition 13.20. *Let N be the number of G_k-orbits $O \in T/G_k$ with $\prod_{\mathfrak{s} \in O} \epsilon_{\mathfrak{s}}(F) = -1$. Then, we have*

$$\dim \mathfrak{B}_{C/K}[2] \equiv \begin{cases} N + 1 \ (mod \ 2) & \epsilon_{\mathcal{R}}(F) = -1, \ g \ even, \ all \ \mathfrak{s} \in B \setminus T \ have \ |Orb_{\mathfrak{s}}| \ even, \\ N \ (mod \ 2) & otherwise. \end{cases}$$

We begin with the following lemma which will be needed during the proof.

Lemma 13.21. *Suppose that* $B \neq \emptyset$ *and that all* $\mathfrak{s} \in B \setminus T$ *have* $|Orb_{\mathfrak{s}}|$ *even. Then*

$$|B \cap T| \equiv g - 1 \ (\text{mod} \ 2).$$

Proof. Note that the assumption that B is non-empty means that $\mathcal{R}$ is übereven. Let $\mathfrak{s} \neq \mathcal{R}$ be a proper cluster with $\mathfrak{s} \notin B \cap T$. We claim that $|\mathrm{Orb}_{\mathfrak{s}}|$ is even. Indeed, the assumptions on $\mathfrak{s}$ mean, in particular, that $\mathfrak{s}$ is contained in a child $\mathfrak{s}'$ of $\mathcal{R}$. Clearly, $\mathfrak{s}'$ cannot be in T. Thus, $\mathfrak{s}' \in B \setminus T$; hence, $|\mathrm{Orb}_{\mathfrak{s}'}|$ is even by assumption. Since $\mathfrak{s} \subseteq \mathfrak{s}'$, it follows that $|\mathrm{Orb}_{\mathfrak{s}}|$ is even also, proving the claim. Next, combining Theorem 13.19 and [18, Theorem 1.10] with [29, Lemma 10.3.18] gives

$$g = \mathrm{rk}\Lambda + \sum_{\mathfrak{s} \ \mathrm{principal}} g(\mathfrak{s}). \tag{13.22}$$

The assumption that $B \neq \emptyset$ means that either $\mathcal{R}$ is non-principal or $g(\mathcal{R}) = 0$. Thus, each principal cluster of positive genus has an even-sized G_k-orbit, so the second term on the right-hand side of Equation 13.22 is an even integer. We therefore have

$$|A| - 1 = \mathrm{rk}\Lambda \equiv g \ (\text{mod} \ 2).$$

By the initial claim, every cluster $\mathfrak{s} \in A$ has $|\mathrm{Orb}_{\mathfrak{s}}|$ even, save possibly for those clusters in $B \cap T$. Thus, $|A| \equiv |B \cap T| \pmod{2}$ and the result follows. $\qquad\square$

Proof of Proposition 13.20. We will deduce the result from Proposition 12.18.

Case 1: either $B = \emptyset$, **or** $B \neq \emptyset$ **and** $\epsilon_{\mathcal{R}}(F) = 1$. Consider the element $t = \sum_{\mathfrak{s} \in T} \ell_{\mathfrak{s}}$ of Π. By Lemma 13.17, for all $\lambda \in \Lambda$, we have

$$\langle \lambda, \lambda \rangle \equiv \langle \lambda, t \rangle \pmod{2}.$$

Further, we have

$$Ft - t = \sum_{\mathfrak{s} \in T} (\epsilon_{F^{-1}\mathfrak{s}}(F) - 1) \ell_{\mathfrak{s}}.$$

It follows that $Ft - t \in 2\Lambda$ (note that if $B \neq \emptyset$, then for any $\mathfrak{s} \in T \cap B$, we have $\epsilon_{F^{-1}\mathfrak{s}}(F) = \epsilon_{\mathcal{R}}(F) = 1$). Taking $x = t$ in Proposition 12.18 then gives

$$\dim \mathfrak{B}_{C/K}[2] \equiv \left\langle \sum_{\mathfrak{s} \in T} \ell_{\mathfrak{s}}, \ \sum_{\mathfrak{s} \in T} \tfrac{1}{2}(\epsilon_{F^{-1}\mathfrak{s}}(F) - 1) \ell_{\mathfrak{s}} \right\rangle \pmod{2}$$

$$\equiv \#\{\mathfrak{s} \in T \ : \ \epsilon_{\mathfrak{s}}(F) = -1\} \pmod{2},$$

the last congruence following from Lemma 13.17.[†] Thus, we have the result in this case.

Case 2: $B \neq \emptyset$, $\epsilon_{\mathcal{R}}(F) = -1$, $|B \cap T|$ **even.** Write $B \cap T = \{\mathfrak{s}_1, \ldots, \mathfrak{s}_{2k}\}$. This time we set $t = \sum_{\mathfrak{s} \in T \backslash B} \ell_{\mathfrak{s}} + \sum_{i=1}^{2k} (-1)^i \ell_{\mathfrak{s}_i}$, noting that $t \in \Lambda$. As with the previous case, taking $x = t$ in Proposition 12.18 gives the result (note that by Lemma 13.21, we are trying to show that $\dim \mathfrak{B}_{C/K}[2] \equiv N \pmod{2}$ in this case).

Case 3: $B \neq \emptyset$, $\epsilon_{\mathcal{R}}(F) = -1$, $|B \cap T|$ **odd,** $|\mathrm{Orb}_{\mathfrak{s}}|$ **odd for some** $\mathfrak{s} \in B \backslash T$. Choose some $\mathfrak{s}_1 \in B \backslash T$ with $m_1 = |\mathrm{Orb}_{\mathfrak{s}_1}|$ odd, and write $m_2 = |B \cap T|$. This time, take

$$t = \sum_{\mathfrak{s} \in T \backslash B} \ell_{\mathfrak{s}} + m_1 \cdot \sum_{\mathfrak{s} \in T \cap B} \ell_{\mathfrak{s}} - m_2 \cdot \sum_{\mathfrak{s} \in \mathrm{Orb}_{\mathfrak{s}_1}} \ell_{\mathfrak{s}_1},$$

which lies in Λ by construction. Again, we conclude by taking $x = t$ in Proposition 12.18.

Case 4: $B \neq \emptyset$, $\epsilon_{\mathcal{R}}(F) = -1$, $|B \cap T|$ **odd, all** $\mathfrak{s} \in B \backslash T$ **have** $|\mathrm{Orb}_{\mathfrak{s}}|$ **even.** Note that in this case, we have g even by Lemma 13.21, so we want to show that $\dim \mathfrak{B}_{C/K}[2] \equiv N + 1 \pmod{2}$. Since each $\mathfrak{s} \in B \backslash T$ has $|\mathrm{Orb}_{\mathfrak{s}}|$ even, we can partition $B \backslash T$ into two disjoint sets B_0 and B_1 with $F(B_0) = B_1$. For $\mathfrak{s} \in A$, write $\ell_{\mathfrak{s}}^{\vee}$ for the element of $\mathrm{Hom}(\Lambda, \mathbb{Z})$ sending $\ell_{\mathfrak{s}}$ to 1, and sending $\ell_{\mathfrak{s}'}$ to 0 for each $\mathfrak{s}' \neq \mathfrak{s}$. Consider the element

$$\phi = \left\langle \sum_{\mathfrak{s} \in T \backslash B} \ell_{\mathfrak{s}}, - \right\rangle + \sum_{\mathfrak{s} \in B_0} \ell_{\mathfrak{s}}^{\vee} - \sum_{\mathfrak{s} \in B_1} \ell_{\mathfrak{s}}^{\vee} \ \in \mathrm{Hom}(\Lambda, \mathbb{Z}).$$

[†] When $|T \cap B|$ is odd, the element t of Π is not in Λ, so Proposition 12.18 does not naively apply. However, in this case, we can take $\phi = \langle t, - \rangle \in \mathrm{Hom}(\Lambda, \mathbb{Z})$ in Remark 12.20 to see that the conclusion concerning $\dim \mathfrak{B}_{C/K}[2]$ remains valid.

Then we have $\langle \lambda, \lambda \rangle \equiv \phi(\lambda) \pmod 2$, as follows from Lemma 13.17 upon noting that Λ is by definition the collection of elements $\sum_{\mathfrak{s}} n_{\mathfrak{s}} \ell_{\mathfrak{s}} \in \Pi$ for which $\sum_{\mathfrak{s} \in B} n_{\mathfrak{s}} = 0$. Moreover, we have

$$F\phi - \phi = \left\langle \sum_{\mathfrak{s} \in T \backslash B} (\epsilon_{F^{-1}\mathfrak{s}}(F) - 1)\ell_{\mathfrak{s}}, - \right\rangle.$$

Since $\sum_{\mathfrak{s} \in T \backslash B}(\epsilon_{F^{-1}\mathfrak{s}}(F) - 1)\ell_{\mathfrak{s}} \in 2\Lambda$, we can apply Remark 12.20 to ϕ, giving

$$\dim \mathfrak{B}_{C/K}[2] \equiv \phi\left(\frac{1}{2} \sum_{\mathfrak{s} \in T \backslash B} (\epsilon_{F^{-1}\mathfrak{s}}(F) - 1)\ell_{\mathfrak{s}} \right) \pmod 2$$

$$\equiv \#\{\mathfrak{s} \in T \backslash B : \epsilon_{\mathfrak{s}}(F) = -1\} \pmod 2.$$

This latter quantity is congruent to $N + 1$ modulo 2. Indeed, every element of $B \cap T$ has $\epsilon_{\mathfrak{s}}(F) = -1$ by assumption. Since moreover $|B \cap T|$ is assumed odd, the claimed congruence follows. □

Remark 13.23. Instead of appealing to Proposition 12.18, an alternative approach to proving Proposition 13.20 might be to draw on work of Betts [3, Section 3] (see also [2, Section 10]), which gives a description in terms of clusters for the individual Tamagawa numbers $c(J/L)$ and $c(J/K)$. From this, one might then hope to prove the result by computing explicitly the quotient $c(J/L)/c(J/K)$ and appealing to (11.8). However, the description of Tamagawa numbers given in that work becomes sufficiently complicated in the presence of übereven clusters that we have elected to avoid this approach.

Before stating the final result of the section, we require one further piece of notation.

Notation 13.24. Define $\kappa(C) \in \{0, 1\}$ as follows. We set $\kappa(C) = 1$ if $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of 2 odd G_k-conjugate clusters $\mathfrak{s}_1$ and $\mathfrak{s}_2$ with both δ_{s_1} and δ_{s_2} odd (note in particular that this forces C to have even genus). We set $\kappa(C) = 0$ otherwise.

Corollary 13.25. *We have*

$$\dim \mathfrak{B}_{C/K}[2] + \epsilon(C/K) \equiv \kappa(C) + \#\left\{ G_k\text{-orbits } O \subseteq T \text{ with } \prod_{\mathfrak{t} \in O} \epsilon_{\mathfrak{t}}(F) = -1 \right\} \pmod 2.$$

Proof. Combine Proposition 13.20 with [18, Theorem 1.23] (the cited result gives an explicit description of deficiency in terms of clusters; to apply it, recall that we have a running assumption that $\mathcal{R}$ has no cotwins). □

14 | RAMIFIED QUADRATIC TWISTS OF SEMISTABLE HYPERELLIPTIC CURVES

We retain the notation and setup of the previous section. Thus, K is a non-archimedean local field of odd residue characteristic, and $C/K : y^2 = f(x)$ is a semistable hyperelliptic curve over K. We continue to impose Assumption 13.4, so that $f(x)$ has even degree and the set $\mathcal{R}$ of roots of $f(x)$

in $\bar{K}$ has no cotwins in the sense of Definition 13.2. Let L/K be a ramified quadratic extension of K, and write $L = K(\sqrt{\pi})$ for some uniformiser $\pi \in K$.

14.1 | The minimal regular model of C^L

We now give an explicit 'cluster picture' description of the special fibre of the minimal regular model of the quadratic twist $C^L : y^2 = \pi f(x)$ of C by L. As we shall see, even though C^L is no longer semistable over K, one can still give a simple description of its minimal regular model in terms of clusters. To avoid confusion when comparing invariants of C with invariants of C^L later, we will make the following convention.

Convention 14.1. Unless stated otherwise, in this section, we will view all clusters as being associated to the polynomial $f(x)$ defining C, as opposed to the polynomial $\pi f(x)$ defining C^L. Since both the clusters themselves and the associated functions $d_{\mathfrak{s}}$ and δ_s (depth and relative depth) are functions purely of the set of roots $\mathcal{R}$, they are unchanged under replacing $f(x)$ by $\pi f(x)$. Thus, the distinction here is irrelevant. However, for a cluster $\mathfrak{s}$, the functions $\nu_{\mathfrak{s}}$ and $\epsilon_{\mathfrak{s}}$ (see (13.7), Definition 13.11) are defined with reference to the leading coefficient of the polynomial in question, and hence may change upon replacing $f(x)$ by $\pi f(x)$. For example, for a proper cluster $\mathfrak{s}$, $\nu_{\mathfrak{s}}$ is one larger when $\mathfrak{s}$ is viewed as a cluster for C^L than when it is viewed as a cluster for C.

In several statements below, we will need to distinguish the following special case.

Notation 14.2. We say that $\mathcal{R}$ is *atypical* if $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of 2 odd proper clusters $\mathfrak{s}_1$ and $\mathfrak{s}_2$, with both $\delta_{\mathfrak{s}_1}$ and $\delta_{\mathfrak{s}_2}$ odd.

The description of the special fibre of the minimal regular model of C^L that we present below follows from work of Faraggi–Nowell [20], which more generally gives an explicit description of the special fibre of the minimal regular SNC model for hyperelliptic curves with tame reduction (i.e. attaining semistable reduction after a tamely ramified extension of the base field). As is apparent from the statement of Proposition 14.5 below, their description simplifies significantly for quadratic twists of semistable hyperelliptic curves. We caution that [20] contains some minor errors. These are discussed and corrected in the PhD thesis of Nowell [45] (see also [2, Section 9]).

Remark 14.3. For an alternative, but related, approach to constructing regular models of hyperelliptic curves over non-archimedean local fields of odd residue characteristic, see the works of Srinivasan [59] and Obus–Srinivasan [46].

In what follows we denote by $\mathcal{X}$ the minimal regular model of C^L over $\mathcal{O}_K$, and denote by $\mathcal{X}_{\bar{k}}$ its special fibre, base-changed to $\bar{k}$.

Notation 14.4. In describing $\mathcal{X}_{\bar{k}}$, we will use the following terminology; see [20, Definition 3.1] for more details. By a chain of n rational curves of multiplicity d, $n \geqslant 0$, $d \geqslant 1$, we mean a collection of irreducible components $\Gamma_1, \ldots, \Gamma_n$ of $\mathcal{X}_{\bar{k}}$, each isomorphic to $\mathbb{P}^1_{\bar{k}}$, such that Γ_i intersects Γ_{i+1} transversally for each i, and such that each Γ_i has multiplicity d in $\mathcal{X}_{\bar{k}}$. We depict this situation below. By a crossed tail, we mean a chain of rational curves $\Gamma_1, \ldots, \Gamma_n$, along with two additional

irreducible components, the 'crosses', both isomorphic to $\mathbb{P}^1_{\bar{k}}$ and intersecting Γ_n transversally. Again, this situation is depicted below. In all the crossed tails we consider, each Γ_i has multiplicity 2, whilst the crosses have multiplicity 1.
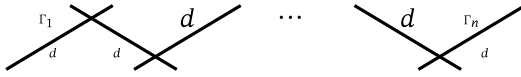
Chain of n rational curves of multiplicity d
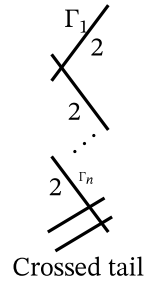
Crossed tail

The promised description of $\mathcal{X}_{\bar{k}}$ is as follows.

Proposition 14.5. *All irreducible components of $\mathcal{X}_{\bar{k}}$ intersect transversally, and no three components intersect at a point. Moreover:*

- *every principal cluster $\mathfrak{s}$ for C contributes to $\mathcal{X}_{\bar{k}}$ a single component $\Gamma_{\mathfrak{s}}$ of genus 0 and multiplicity 2,*
- *components corresponding to principal clusters $\mathfrak{s}' < \mathfrak{s}$ are linked by:*
  - *a chain of $\frac{1}{2}\delta_{\mathfrak{s}'}$ rational curves of multiplicity 1 if $\mathfrak{s}'$ is odd,*
  - *a chain of $(2\delta_{\mathfrak{s}'} - 1)$ rational curves of multiplicity 2 if $\mathfrak{s}'$ is even,*
- *for $\mathfrak{s}$ principal, each twin $\mathfrak{t} < \mathfrak{s}$ contributes a crossed tail $T_{\mathfrak{t}}$ whose first component intersects $\Gamma_{\mathfrak{s}}$, and which consists of $2\delta_{\mathfrak{t}}$ rational curves of multiplicity 2, with the crosses having multiplicity 1,*
- *if $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ and both $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are odd, then $\Gamma_{\mathfrak{s}_1}$ and $\Gamma_{\mathfrak{s}_2}$ are linked by a chain of $\frac{1}{2}(\delta_{\mathfrak{s}_1} + \delta_{\mathfrak{s}_2})$ rational curves of multiplicity 1,*
- *if $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ and both $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are even, then $\Gamma_{\mathfrak{s}_1}$ and $\Gamma_{\mathfrak{s}_2}$ are linked by a chain of $2\delta_{\mathfrak{s}_1} + 2\delta_{\mathfrak{s}_2} - 1$ rational curves of multiplicity 2,*
- *for a principal cluster $\mathfrak{s}$, each child of size 1, $\{r\} < \mathfrak{s}$ say, contributes a single rational curve T_r of multiplicity 1, intersecting $\Gamma_{\mathfrak{s}}$.*

As mentioned, Proposition 14.5 will follow from results of Faraggi and Nowell, specifically from [20, Theorems 7.12 and 7.18] and [45, Theorems 9.23, 9.31 and 9.32]. These results take as input several invariants of hyperelliptic curves. In the case in hand, we describe these invariants in Lemma 14.7 below.

Caution 14.6. In Lemma 14.7 only, we view clusters as being associated to $\pi f(x)$ rather than $f(x)$, since it is invariants of the former which constitute the required input for the results of [20] and [45].

See [20, Table 3] and the references therein for the definitions of the invariants appearing in the statement of Lemma 14.7 below. Briefly, for a proper cluster $\mathfrak{s}$ for C^L, the quantities $d_{\mathfrak{s}}$, $\nu_{\mathfrak{s}}$ and $\delta_{\mathfrak{s}}$ are as defined in Section 13.1, but with $\pi f(x)$ in place of $f(x)$. By definition, we have $\lambda_{\mathfrak{s}} = \frac{1}{2}\nu_{\mathfrak{s}} - d_{\mathfrak{s}} \sum_{\mathfrak{s}' < \mathfrak{s}} \lfloor \frac{|\mathfrak{s}'|}{2} \rfloor$ (we caution that this is the function denoted as $\tilde{\lambda}_{\mathfrak{s}}$ in [18, Notation 1.19]). The quantity $e_{\mathfrak{s}}$ is the minimal positive integer such that both $e_{\mathfrak{s}} d_{\mathfrak{s}} \in \mathbb{Z}$ and $e_{\mathfrak{s}} \nu_{\mathfrak{s}} \in 2\mathbb{Z}$.

When $\mathfrak{s}$ is even, the *invariant* $\epsilon_{\mathfrak{s}} \in \{\pm 1\}$ in the statement is given by evaluating the *function* $\epsilon_{\mathfrak{s}}$ of Definition 13.11 (which no longer factors through G_k in general since C^L/K is not semistable) at any topological generator of the tame inertia group of K. For our purposes, we may take as a definition that $\epsilon_{\mathfrak{s}} = (-1)^{\nu_{\mathfrak{s}*} - |\mathfrak{s}*| d_{\mathfrak{s}*}}$ for $\mathfrak{s}*$ as in Notation 13.10. We will not use this variant of $\epsilon_{\mathfrak{s}}$ anywhere else in the paper. Recall from Notation 13.8 the definition of the set T.

Lemma 14.7. *Let $\mathfrak{s}$ be a proper cluster for C^L (i.e. for the polynomial $\pi f(x)$). Then $\mathfrak{s}$ is fixed by the inertia group I_K of K, and all of the following hold:*

(i) *we have $d_{\mathfrak{s}} \in \mathbb{Z}$ unless $\mathfrak{s} \in T$, in which case $d_{\mathfrak{s}} \in 1/2 + \mathbb{Z}$,*
(ii) *$\nu_{\mathfrak{s}}$ is odd unless either $\mathfrak{s} = \mathcal{R}$ and $\mathcal{R}$ is atypical, or $\mathfrak{s} \in T$. In these cases, $\nu_{\mathfrak{s}}$ is even.*
(iii) *if $\mathfrak{s}$ is even, then $\epsilon_{\mathfrak{s}} = -1$ unless $\mathfrak{s} = \mathcal{R}$ is atypical, in which case $\epsilon_{\mathfrak{s}} = 1$,*
(iv) *if $|\mathfrak{s}| \geqslant 3$, then $e_{\mathfrak{s}} = 2$ unless $\mathfrak{s} = \mathcal{R}$ is atypical, in which case $e_{\mathfrak{s}} = 1$,*
(v) *if $\mathfrak{s}$ is principal, then $\lambda_{\mathfrak{s}} \in \frac{1}{2} + \mathbb{Z}$,*
(vi) *if $\mathfrak{s}' < \mathfrak{s}$ are principal clusters with $\mathfrak{s}'$ odd, then $\delta_{\mathfrak{s}'}$ is even.*

Proof. As noted above, the proper clusters for C^L and their associated depths are the same as those for C (and whether or not a cluster $\mathfrak{s}$ is proper/principal/odd/even/übereven is similarly independent of whether we view $\mathfrak{s}$ as a cluster for C or C^L). However, given a cluster $\mathfrak{s}$ for C, when we view it as a cluster for C^L the quantity $\nu_{\mathfrak{s}}$ increases by 1 since the leading coefficient of $\pi f(x)$ has valuation one greater than that of $f(x)$. All claims are now a formal consequence of Theorem 13.6, which applies since $C : y^2 = f(x)$ is semistable. Explicitly, the claim that each I_K-orbit of proper clusters has size 1 is part (2) of Theorem 13.6. Part (i) is Lemma 13.9. Part (ii) for $\mathfrak{s} \notin T$ is [18, Lemma 4.7], whilst for $\mathfrak{s} \in T$, this follows from [18, Lemma C.5], combined with [18, Lemma 4.7] applied to the parent of $\mathfrak{s}$. Parts (iii) and (iv) follow from parts (i) and (ii). Part (v) follows from (ii). Finally, for part (vi), see [18, Lemma C.7]. $\square$

Proof of Proposition 14.5. It suffices to show that the special fibre of the minimal regular SNC model of C^L, base-changed to $\bar{k}$, admits the description given in the statement. Indeed, the claimed description of the special fibre visibly contains no exceptional curves, thus having shown that the special fibre of the minimal regular SNC model admits this description, it follows that the minimal regular SNC model coincides with the minimal regular model in this case.

With the relevant invariants being described by Lemma 14.7, that the minimal regular SNC model takes the desired form now follows from specialising [20, Theorems 7.12 and 7.18] to the case in hand, save for the fact that the statements of these results contain some minor errors. A corrected version of the relevant results appears in the PhD thesis of Nowell [45, Theorems 9.23, 9.31 and 9.32] (see also [2, Section 9]), from which one obtains the claimed description of the minimal regular SNC model. $\square$

It is convenient to package the description of $\mathcal{X}_{\bar{k}}$ given in Proposition 14.5 in terms of the following graph.

Notation 14.8. Define $\mathcal{T}$ to be the graph consisting of one vertex for each irreducible component of $\mathcal{X}_{\bar{k}}$, with vertices v and v' joined by an edge if and only if the corresponding components intersect. We give each vertex a weight $d_v \in \{1, 2\}$ according to the multiplicity of the corresponding component in $\mathcal{X}_{\bar{k}}$.

Remark 14.9. We see from Proposition 14.5 that $\mathcal{T}$ is a connected tree. Note that any vertex of $\mathcal{T}$ of degree at least 3 has weight 2. The leaves of $\mathcal{T}$ correspond to the components Γ_r for $r \in \mathcal{R}$ not in a twin, along with the 'crosses' on the crossed tails $T_\mathfrak{t}$ for twins $\mathfrak{t}$. In particular, $\mathcal{T}$ has $|\mathcal{R}| = 2g + 2$ leaves. Moreover, each leaf has weight 1.

Example 14.10 (Ramified quadratic twist of good reduction). Suppose $f(x) \in \mathcal{O}_K[x]$ is monic, has degree $2g + 2$ for some $g \geqslant 2$ and is such that the reduction $f(x) \pmod{\pi}$ is separable. Then $C : y^2 = f(x)$ has good reduction, and C^L/K is the hyperelliptic curve $C^L : y^2 = \pi f(x)$. We now use Proposition 14.5 to describe $\mathcal{X}_{\bar{k}}$ in this case. The assumptions mean that $f(x)$ has a single proper cluster, given by the full set of roots $\mathcal{R}$. This cluster has depth 0 and has $2g + 2$ children, with each individual root $r \in \mathcal{R}$ contributing a child $\{r\} < \mathcal{R}$ of size 1. The cluster picture is thus the following:

By Proposition 14.5, $\mathcal{X}_{\bar{k}}$ consists of one component $\Gamma_{\mathcal{R}}$ of genus 0 and multiplicity 2, intersected transversely by $2g + 2$ rational curves of multiplicity 1, one for each root $r \in \mathcal{R}$, as depicted below. The graph $\mathcal{T}$ consists of $2g + 2$ vertices of weight 1, each joined to a common vertex $v_{\mathcal{R}}$ of weight 2, as shown below also. In the picture, we do not label multiplicities/weights unless they are greater than 1.
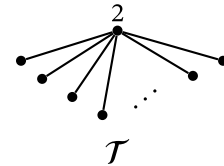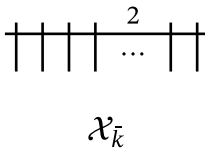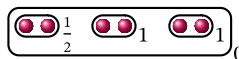

This description of $\mathcal{X}_{\bar{k}}$ is consistent with work of Sadek [55, Theorem 3.7].

Example 14.11. Take C to be the semistable genus 2 hyperelliptic curve over $\mathbb{Q}_3$ considered previously in 9.12, 13.3, and take $L = \mathbb{Q}_3(\sqrt{3})$, so that C^L is the curve

$$C^L/\mathbb{Q}_3 : y^2 = 3(x^2 + 3)((x - i)^2 - 3^2)((x + i)^2 - 3^2)$$

for i a square root of -1. As in Example 13.3, the cluster picture is as shown:

As explained previously in Example 13.3, the full set of roots $\mathcal{R}$ is the unique principal cluster, and (as shown in the picture) there are three twins $\mathfrak{t}_1$, $\mathfrak{t}_2$ and $\mathfrak{t}_3$, with $\delta_{\mathfrak{t}_1} = 1/2$ and $\delta_{\mathfrak{t}_2} = \delta_{\mathfrak{t}_3} = 1$. By Proposition 14.5, $\mathcal{X}_{\bar{k}}$ consists of one component $\Gamma_{\mathcal{R}}$ of multiplicity 2, along with three crossed tails,

as depicted below. The corresponding graph $\mathcal{T}$ is pictured also.

In particular, in the terminology of the Namikawa–Ueno classification [43], C^L/K has type I^*_{1-2-2}.

Returning to the general case, we now describe the G_k-action on the set of irreducible components of $\mathcal{X}_{\bar{k}}$ (equivalently the induced G_k-action on $\mathcal{T}$). To do this, we introduce the following notation.

Notation 14.12. For each twin $\mathfrak{t} = \{r_1, r_2\}$, let $\eta_{\mathfrak{t}} \in K^{s\times}$ be a choice of square root of

$$\frac{(r_1 - r_2)^2}{(-\pi)^{2d_{\mathfrak{t}}}},$$

noting that $d_{\mathfrak{t}} = v(r_1 - r_2)$ so that the displayed quantity is a unit (we can have $d_{\mathfrak{t}} \in \frac{1}{2} + \mathbb{Z}$, so we need not have a canonical choice of square root). In particular, $\eta_{\mathfrak{t}} \in \mathcal{O}^{\times}_{K^{\mathrm{nr}}}$. Define the function $\gamma_{\mathfrak{t},L} : G_K \to \{\pm 1\}$ by the formula

$$\gamma_{\mathfrak{t},L}(\sigma) = \frac{\sigma(\eta_{\mathfrak{t}})}{\eta_{\sigma\mathfrak{t}}}.$$

The function $\gamma_{\mathfrak{t},L}$ factors through $\mathrm{Gal}(K^{\mathrm{nr}}/K)$. Thus, we view $\gamma_{\mathfrak{t},L}$ as a function on G_k as well. In particular, we can speak about $\gamma_{\mathfrak{t},L}(F)$ where $F \in G_k$ is the Frobenius element. The function $\gamma_{\mathfrak{t},L}$ may depend on the choice of square root $\eta_{\mathfrak{t}}$, but its restriction to the stabiliser of $\mathfrak{t}$ does not. We remark that we include L in the notation for $\gamma_{\mathfrak{t},L}$ since, when $d_{\mathfrak{t}} \in 1/2 + \mathbb{Z}$, it depends on the class of the uniformiser π in $K^{\times}/K^{\times 2}$.

We stress that Convention 14.1 is in place, which is relevant for the function $\epsilon_{\mathfrak{z}}$.

Proposition 14.13. *Let $\sigma \in G_k$. The action of σ on the set of irreducible components of $\mathcal{X}_{\bar{k}}$ is determined by:*

- *for $\mathfrak{z}$ principal, the component $\Gamma_{\mathfrak{z}}$ is sent to $\Gamma_{\sigma\mathfrak{z}}$,*
- *for each $r \in \mathcal{R}$ not in a twin, the component Γ_r is sent to $\Gamma_{\sigma r}$,*
- *for a twin $\mathfrak{t}$ with $\mathfrak{t} \notin T$, the crossed tail $T_{\mathfrak{t}}$ is sent to $\gamma_{\mathfrak{t}}(\sigma) T_{\sigma\mathfrak{t}}$,[†]*
- *for a twin $\mathfrak{t} \in T$, the crossed tail $T_{\mathfrak{t}}$ is sent to $\epsilon_{\mathfrak{t}}(\sigma) \gamma_{\mathfrak{t}}(\sigma) T_{\sigma\mathfrak{t}}$.*

[†] Here $-T_{\mathfrak{t}}$ denotes the crossed tail $T_{\mathfrak{t}}$ with crosses swapped; strictly speaking we should fix a labelling $\pm$ of the crosses to pin down the action, and this choice is closely related to the choices of square root in Notation 14.12 above. However, it

Proof. This essentially follows from [20, Theorem 7.21]; however, in some cases, the Frobenius action is not correctly computed in that work. The argument given in loc. cit. applies to show that the action is as claimed in the first two bullet points. However, for a crossed tail $T_\mathfrak{t}$ corresponding to a twin $\mathfrak{t}$, the computation given there is incorrect. We explain now how to correctly compute the action in this case.

Since C is semistable over K, the curve C^L becomes semistable over L. The results of [18] then apply to give an explicit description of the minimal proper regular model $\widetilde{\mathcal{X}}/\mathcal{O}_{L^\mathrm{ur}}$ of C^L/L^ur in terms of clusters for C^L and their associated invariants. In particular, equations for the components of the special fibre $\widetilde{\mathcal{X}}_{\bar{k}}$ can be read off from [18, Proposition 5.20]. By uniqueness of the minimal regular model, the full Galois group G_K acts semilinearly on $\widetilde{\mathcal{X}}_{\bar{k}}$, and this action factors through $\mathrm{Gal}(L^\mathrm{ur}/K)$. This action is described explicitly in terms of clusters in [18, Theorem 6.2]. Writing $G = \mathrm{Gal}(L^\mathrm{ur}/K^\mathrm{nr})$, the quotient $\widetilde{\mathcal{X}}/G$ is an $\mathcal{O}_{K^\mathrm{nr}}$-model for C^L, closely related to its minimal regular model. In particular, as explained in the proof of [20, Theorem 7.21], the G_k-action on the crossed tails of $\mathcal{X}_{\bar{k}}$ can be read off from the G_k-action on the singular points of the special fibre of $\widetilde{\mathcal{X}}/G$, which can, in turn, be calculated using the results of [18] mentioned above. To carry out this calculation, fix a twin $\mathfrak{t} = \{r_1, r_2\}$. We take as a centre for $\mathfrak{t}$ the quantity $z_\mathfrak{t} := \frac{r_1 + r_2}{2} \in K^\mathrm{nr}$. As described in [18, Proposition 5.20], associated to $\mathfrak{t}$ is the component $\Gamma_\mathfrak{t}$ of $\widetilde{\mathcal{X}}_{\bar{k}}$, given by the equation

$$\Gamma_\mathfrak{t} : y^2 = c_\mathfrak{t}\left(x^2 - \frac{(r_1 - r_2)^2}{4\pi^{2d_\mathfrak{t}}} \bmod \mathfrak{m}\right) \quad \text{for} \quad c_\mathfrak{t} = \frac{c_f}{\pi^{v(c_f)}} \prod_{r \in \mathcal{R} \setminus \mathfrak{t}} \left(\frac{z_\mathfrak{t} - r}{\pi^{v(z_\mathfrak{t} - r)}}\right) \bmod \mathfrak{m}.$$

Here $\mathfrak{m}$ denotes the maximal ideal in $\mathcal{O}_{\bar{K}}$ and 'mod $\mathfrak{m}$' denotes reduction to the residue field $\bar{k}$. Recall that $2d_\mathfrak{t} \in \mathbb{Z}$ is odd if $\mathfrak{t} \in T$, and is even otherwise. Using the description of the invariant $v_\mathfrak{t}$ afforded by Lemma 14.7 (ii), we see from [18, Theorem 6.2] that the generator τ of G acts on $\Gamma_\mathfrak{t}$ as the automorphism

$$(x, y) \longmapsto \begin{cases} (x, -y) & \mathfrak{t} \notin T, \\ (-x, y) & \mathfrak{t} \in T. \end{cases}$$

The relevant singular points of the special fibre of $\widetilde{\mathcal{X}}/G$ arise as the image under the quotient map of the fixed points of the action of τ on $\Gamma_\mathfrak{t}$. These are the points $P_\mathfrak{t}^\pm \in \Gamma_\mathfrak{t}$ given by

$$P_\mathfrak{t}^\pm = \left(\pm\tfrac{1}{2}\overline{\eta_\mathfrak{t}}, 0\right) \text{ if } \mathfrak{t} \notin T \quad \text{and} \quad P_\mathfrak{t}^\pm = \left(0, \pm\tfrac{1}{2}\overline{\eta_\mathfrak{t}}\sqrt{c_\mathfrak{t}}\right) \text{ if } \mathfrak{t} \in T,$$

where here $\overline{\eta_\mathfrak{t}} := \eta_\mathfrak{t} \bmod \mathfrak{m}$. Since the points $P_\mathfrak{t}^\pm$ are fixed by G, the action of $\mathrm{Gal}(L^\mathrm{ur}/K)$ on these points descends to an action of $\mathrm{Gal}(K^\mathrm{nr}/K) = G_k$, and appealing to [18, Theorem 6.2] once more to determine this action, we see that $\sigma \in G_k$ sends $P_\mathfrak{t}^\pm \in \Gamma_\mathfrak{t}$ to the point on $\Gamma_{\sigma\mathfrak{t}}$ given by acting coordinatewise on the expression for $P_\mathfrak{t}^\pm$ given above. Now the points $P_\mathfrak{t}^\pm$ can be identified with the 'crosses' on the crossed tail $T_\mathfrak{t}$ (cf. proof of [20, Theorem 7.21]). We thus see that the action is as claimed upon noting that, after making compatible choices of square roots, we have $\epsilon_\mathfrak{t}(\sigma) = \sigma(\sqrt{c_\mathfrak{t}})/\sqrt{c_{\sigma\mathfrak{t}}}$ (to justify this final equality, see [18, Lemma 6.7] and the surrounding discussion). $\qquad\square$

---

will only be relevant in what follows to know whether the stabiliser of a twin $\mathfrak{t}$ fixes or swaps the crosses on $T_\mathfrak{t}$, and for this, we can safely ignore this subtlety.

Remark 14.14. In Remark 14.9, we described the leaves of $\mathcal{T}$. From Proposition 14.13, we see that leaves corresponding to roots $r \in \mathcal{R}$ not lying in a twin are permuted by G_k as the corresponding roots are. Further, let us temporarily denote by $\mathcal{S}$ the subset of $\mathcal{R}$ consisting of roots lying in twins $\mathfrak{t}$ with $\mathfrak{t} \notin T$, noting that $\mathcal{S} \subseteq \mathcal{R} \cap K^{\mathrm{nr}}$. If we further denote by $\mathcal{L}$ the set of leaves corresponding to the 'crosses' on the crossed tails $T_{\mathfrak{t}}$ for $\mathfrak{t} \notin T$, then we see from Proposition 14.13 that $\mathcal{L}$ and $\mathcal{S}$ are isomorphic as G_k-sets.

Example 14.15. Returning to Example 14.11, for all $\sigma \in G_k$, we have $\epsilon_{\mathfrak{t}_1}(\sigma) = \epsilon_{\mathfrak{t}_2}(\sigma) = \epsilon_{\mathfrak{t}_3}(\sigma) = 1$ (cf. Example 13.14). One checks that we may take the functions $\gamma_{\mathfrak{t}_1}$, $\gamma_{\mathfrak{t}_2}$ and $\gamma_{\mathfrak{t}_3}$ to be identically 1 also. Finally, the Frobenius element in G_k fixes $\mathfrak{t}_1$ but swaps $\mathfrak{t}_2$ and $\mathfrak{t}_3$. We thus see from Proposition 14.13 that F fixes the crossed tail corresponding to $\mathfrak{t}_1$ (the leftmost one in the picture) and swaps the crossed tails corresponding to $\mathfrak{t}_2$ and $\mathfrak{t}_3$. Moreover, F^2 acts trivially on the full set of components, and hence the stabiliser in G_k of $\mathfrak{t}_i$, $i = 2, 3$, acts trivially on the crosses of the corresponding crossed tail.

14.2 | The Tamagawa number up to squares

We now use the description of $\mathcal{T}$ along with its G_k-action, afforded by 14.5, 14.13, to compute the Tamagawa number of J^L/K up to rational squares. We begin by describing the order of the component group over $\bar{k}$.

Lemma 14.16. *We have* $|\Phi(\bar{k})| = 2^{2g}$.

Proof. Since $\mathcal{T}$ is a tree, [6, Proposition 9.6.6] gives

$$|\Phi(\bar{k})| = \prod_{v \in \mathcal{T}} d_v^{\deg(v)-2} = \frac{\prod_{v \in \mathcal{T}} 2^{\deg(v)-2}}{\prod_{\substack{v \in \mathcal{T} \\ d_v=1}} 2^{\deg(v)-2}},$$

where $\deg(v)$ denotes the degree of the vertex v. Since $\mathcal{T}$ is a connected tree, we have

$$\prod_{v \in \mathcal{T}} 2^{\deg(v)-2} = 2^{\sum_{v \in \mathcal{T}} (\deg(v)-2)} = 1/4.$$

Since any vertex of $\mathcal{T}$ of degree at least 3 has multiplicity 2, we find

$$\prod_{\substack{v \in \mathcal{T} \\ d_v=1}} 2^{\deg(v)-2} = 2^{-\#\{\text{leaves of } \mathcal{T}\}} = 2^{-2g-2},$$

the second equality following from Remark 14.9. $\qquad\square$

We now turn to computing the size of the G_k-invariants of $\Phi(\bar{k})$ up to rational squares, which we will do with the aid of Proposition 10.8. We remark that an alternative approach might be to use the recipe [58, Section 4.2] of Srinivasan for computing the Tamagawa number of a curve in terms of its minimal proper regular model.

In what follows it will be convenient to work exclusively with the graph $\mathcal{T}$. To facilitate this, we transfer the intersection pairing between the components of $\mathcal{X}_{\bar{k}}$ to a pairing on the vertices of $\mathcal{T}$. Since by Proposition 14.5, all components intersect transversally, this pairing has a simple combinatorial description.

Definition 14.17. For vertices v and v' of $\mathcal{T}$, define

$$v \bullet v' = \begin{cases} 0 & v \text{ not adjacent to } v', \\ 1 & v \neq v' \text{ and } v, v' \text{ adjacent}, \\ -\frac{1}{d_v} \sum_{w \neq v} d_w\, v \bullet w & v = v'. \end{cases}$$

Note that if vertices v, v' of $\mathcal{T}$ correspond to components Γ_v and $\Gamma_{v'}$, respectively, then $v \bullet v'$ is the intersection number between Γ_v and $\Gamma_{v'}$. We extend this product bilinearly to the $\mathbb{Q}$-vector space V with basis the vertices of $\mathcal{T}$.

Notation 14.18. For $v \in \mathcal{T}$, denote by r_v the size of the G_k-orbit of v. If r_v is even, write

$$\epsilon_v = v - Fv + \cdots - F^{r_v - 1}v \in V.$$

We now define a matrix M with rows and columns indexed by the even length G_k-orbits of vertices of T as follows. For each even length G_k-orbit O, pick a representative $v_O \in O$. Then the (O, O')-entry of M is defined as

$$M_{O,O'} = \frac{1}{r_{v_O}} \epsilon_{v_O} \bullet \epsilon_{v_{O'}}.$$

The relevance of the above definitions is that, by Proposition 10.8, we have

$$|\det M| \equiv 2^{\epsilon(C^L/K)} \cdot \frac{|\Phi(\bar{k})|}{|\Phi(k)|} \pmod{\mathbb{Q}^{\times 2}}. \tag{14.19}$$

Taking 2-adic valuations in (14.19) and noting that we have $|\Phi(k)| = c(J^L/K)$ by definition, it follows from Lemma 14.16 that we have

$$\mathrm{ord}_2 |\det M| \equiv \epsilon(C^L/K) + \mathrm{ord}_2 c(J^L/K) \pmod{2}. \tag{14.20}$$

Proposition 14.21. *Suppose that either $\mathcal{R}$ is a principal cluster, or $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of two proper clusters $\mathfrak{s}_1$ and $\mathfrak{s}_2$ which are not swapped by G_k. Then*

$$|\det M| = 2^{\#\{\text{ even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\}}.$$

We begin with a lemma, which is a variant of [6, Lemma 9.6.7].

Lemma 14.22. *Let $\mathbb{T}$ be a rooted tree with root R. Let N be a matrix with rational coefficients whose rows and columns are indexed by the vertices of $\mathbb{T}$. Suppose that $N_{v,v'} = 0$ save possibly when either $v = v'$ or when v and v' are adjacent in $\mathbb{T}$. Further, suppose that all rows of N sum to 0, save possibly*

the row corresponding to the root R. Then

$$\det N = \left(\prod_{v \in \mathbb{T}, v \neq R} -N_{v, v_{\text{parent}}} \right) \left(\sum_{v \in \mathbb{T}} N_{R,v} \right),$$

where here for a vertex $v \neq R$ of $\mathbb{T}$, v_{parent} denotes the parent of v in $\mathbb{T}$ (i.e. the vertex adjacent to v on the unique path in $\mathbb{T}$ from v to the root R).

Proof. The strategy of proof is the same as that of [6, Lemma 9.6.7], and is by induction on $n = |\mathbb{T}|$. If $n = 1$, the result is clear, so assume $n > 1$. Let $v \neq R$ be a leaf of $\mathbb{T}$ and order the vertices of $\mathbb{T}$ so that v is the first vertex, and its parent v' is the second (the determinant is independent of the ordering of vertices, this is just to enable us to write down the matrix explicitly). The assumptions on N mean that it has the form

$$N = \begin{pmatrix} -N_{v,v'} & N_{v,v'} & 0 & 0 & 0 \\ N_{v',v} & N_{v',v'} & * & * & * \\ 0 & * & * & * & * \\ 0 & * & * & * & * \\ 0 & * & * & * & * \end{pmatrix}.$$

If $N_{v,v'} = 0$, then $\det N = 0$ is as claimed, so suppose $N_{v,v'} \neq 0$. Adding column 1 to column 2 and then adding $\frac{N_{v',v}}{N_{v,v'}} \cdot$ (row 1) to row 2 does not change the determinant, and transforms the matrix above into the matrix

$$\begin{pmatrix} -N_{v,v'} & 0 & 0 & 0 & 0 \\ 0 & N_{v',v'} + N_{v',v} & * & * & * \\ 0 & * & * & * & * \\ 0 & * & * & * & * \\ 0 & * & * & * & * \end{pmatrix}.$$

Here, all entries indicated by a $*$ remain unchanged from the corresponding entries of N. Let $\widetilde{N}$ be the matrix obtained by removing the first row and column from this matrix, so that $\det N = -N_{v,v'} \det \widetilde{N}$. Letting $\widetilde{\mathbb{T}}$ be the rooted tree obtained from $\mathbb{T}$ by removing the leaf v (with root equal to the root R of $\mathbb{T}$), we see that $\widetilde{N}$ satisfies the hypothesis of the statement with respect to $\widetilde{\mathbb{T}}$. By induction, we have

$$\det N = -N_{v,v'} \det \widetilde{N} = -N_{v,v'} \left(\prod_{x \in \widetilde{\mathbb{T}}, x \neq R} -N_{x, x_{\text{parent}}} \right) \left(\sum_{x \in \widetilde{\mathbb{T}}} \widetilde{N}_{R,x} \right)$$

$$= \left(\prod_{x \in \widetilde{\mathbb{T}}, x \neq R} -N_{x, x_{\text{parent}}} \right) \left(\sum_{x \in \widetilde{\mathbb{T}}} \widetilde{N}_{R,x} \right).$$

The conclude, we claim that

$$\sum_{x \in \widetilde{\mathbb{T}}} \widetilde{N}_{R,x} = \sum_{x \in \mathbb{T}} N_{R,x}.$$

Indeed, when $v' \neq R$, we have $N_{R,v} = 0$, and $\widetilde{N}_{R,x} = N_{R,x}$ for each $x \neq v$. From this, the claim follows readily. On the other hand, when $v' = R$, the identity follows from the fact that $\widetilde{N}_{v',v'} = N_{v',v'} + N_{v',v}$, whilst $\widetilde{N}_{v',x} = N_{v',x}$ for all $x \notin \{v, v'\}$. □

Proof of Proposition 14.21. If $\mathcal{R}$ is principal, denote by R the vertex of $\mathcal{T}$ corresponding to the component $\Gamma_{\mathcal{R}}$. If $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$, denote by R the vertex of $\mathcal{T}$ corresponding to $\Gamma_{\mathfrak{s}_1}$. In either case, R is fixed by G_k and $d_R = 2$. We view $\mathcal{T}$ as a rooted tree with root R. For a vertex $v \neq R$, we denote by $P(v)$ the parent of v in $\mathcal{T}$. We say that v is a child of a vertex w if $w = P(v)$.

Now take a vertex v of $\mathcal{T}$ with r_v even, noting that this forces $v \neq R$. If v' is a child of v, then r_v divides $r_{v'}$. In particular, $r_{v'}$ is even also. In this case, we write $r_{v'} = m_{v'} r_v$, noting that $m_{v'}$ is the number of vertices in the G_k-orbit of v' having parent v. One then computes $\epsilon_v \bullet \epsilon_{v'} = m_{v'} r_v = r_{v'}$, so we have

$$\frac{1}{r_v} \epsilon_v \bullet \epsilon_{v'} = m_{v'} \quad \text{and} \quad \frac{1}{r_{v'}} \epsilon_{v'} \bullet \epsilon_v = 1. \tag{14.23}$$

Moreover, we have $\epsilon_v \bullet \epsilon_v = r_v v \bullet v$, giving

$$\frac{1}{r_v} \epsilon_v \bullet \epsilon_v = -\frac{d_{P(v)}}{d_v} - \frac{1}{d_v} \sum_{v' \text{ child of } v} d_{v'}. \tag{14.24}$$

To make use of these computations, pick compatibly a representative for each even-sized G_k-orbit of vertices in $\mathcal{T}$ in such a way that if v is picked, then for each G_k-orbit containing a child of v, the chosen representative of that orbit is itself a child of v. The subgraph of $\mathcal{T}$ generated by all chosen representatives is a finite disjoint union of connected trees, $\mathcal{T}_1, \ldots, \mathcal{T}_s$ say. Each $\mathcal{T}_i$ is naturally a rooted tree, with root R_i the unique vertex of $\mathcal{T}_i$ closest to R, and we extend the notion of child/parent to $\mathcal{T}_i$. We caution, however, that we reserve the notation $P(v)$ for the parent of a vertex v in the tree $\mathcal{T}$. Now for $1 \leqslant i \leqslant s$, define N_i to be the matrix whose rows and columns are indexed by the vertices of $\mathcal{T}_i$, and such that the (v, v')-entry of N_i is given by

$$(N_i)_{v,v'} = \frac{d_v d_{v'}}{r_v} \epsilon_v \bullet \epsilon_{v'} = \begin{cases} d_v d_{v'} & v \text{ a child of } v' \text{ in } \mathcal{T}_i, \\ m_{v'} d_v d_{v'} & v \text{ parent of } v' \text{ in } \mathcal{T}_i, \\ -d_v d_{P(v)} - \sum_{w \text{ child of } v \text{ in } \mathcal{T}_i} m_w d_v d_w & v = v', \\ 0 & \text{otherwise,} \end{cases} \tag{14.25}$$

the second equality following from (14.23) and (14.24). By construction, we have

$$|\det M| = \prod_{i=1}^{s} \left(|\det N_i| \prod_{v \in \mathcal{T}_i} d_v^{-2} \right).$$

Applying Lemma 14.22 to each of the matrices N_i, we find

$$|\det M| = \prod_{i=1}^{s} \prod_{v \in \mathcal{T}_i} \frac{d_{P(v)}}{d_v}. \tag{14.26}$$

Claim. For each $1 \leqslant i \leqslant s$, we have

$$\prod_{v \in \mathcal{T}_i} \frac{d_{P(v)}}{d_v} = \frac{d_{P(R_i)}}{2} 2^{\#\{\text{leaves of } \mathcal{T} \text{ appearing in } \mathcal{T}_i\}}.$$

Proof of claim. Firstly suppose that $\mathcal{T}_i$ consists of the single vertex R_i. Then R_i is necessarily a leaf in $\mathcal{T}$, hence has weight 1 and parent (in $\mathcal{T}$) of weight 2. Thus, the formula holds in this case.

Now assume that $\mathcal{T}_i$ consists of at least two vertices, and for a vertex v in $\mathcal{T}_i$, let $\deg_{\mathcal{T}_i}(v)$ denote the degree of v when viewed as a vertex of $\mathcal{T}_i$ (as opposed to a vertex of $\mathcal{T}$). Note that a vertex $v \neq R_i$ of $\mathcal{T}_i$ is the parent of $(\deg_{\mathcal{T}_i}(v) - 1)$-many vertices of $\mathcal{T}_i$, whilst R_i is the parent of $\deg_{\mathcal{T}_i}(v)$-many vertices of $\mathcal{T}_i$. Consequently, we have

$$\prod_{v \in \mathcal{T}_i} \frac{d_{P(v)}}{d_v} = d_{R_i} d_{P(R_i)} \prod_{v \in \mathcal{T}_i} d_v^{\deg_{\mathcal{T}_i}(v)-2} = d_{R_i} d_{P(R_i)} \frac{\prod_{v \in \mathcal{T}_i} 2^{\deg_{\mathcal{T}_i}(v)-2}}{\prod_{\substack{v \in \mathcal{T}_i \\ d_v=1}} 2^{\deg_{\mathcal{T}_i}(v)-2}}.$$

Since $\mathcal{T}_i$ is a connected tree, we have

$$\prod_{v \in \mathcal{T}_i} 2^{\deg_{\mathcal{T}_i}(v)-2} = 2^{\sum_{v \in \mathcal{T}_i}(\deg_{\mathcal{T}_i}(v)-2)} = 1/4.$$

On the other hand, if $v \in \mathcal{T}_i$ has $\deg_{\mathcal{T}_i}(v) \geqslant 3$, then v necessarily has degree at least 3 when viewed as a vertex of $\mathcal{T}$. It then follows from the description of $\mathcal{T}$ afforded by Proposition 14.5 that $d_v = 2$. All together, this gives

$$\prod_{v \in \mathcal{T}_i} \frac{d_{P(v)}}{d_v} = \frac{d_{R_i} d_{P(R_i)}}{4} 2^{\#\{v \in \mathcal{T}_i \ : \ \deg_{\mathcal{T}_i}(v)=1, \ d_v=1\}}. \tag{14.27}$$

Under the assumption that $\mathcal{T}_i$ has at least two vertices, we see that a vertex $v \in \mathcal{T}_i$ is a leaf in $\mathcal{T}$ if and only if $\deg_{\mathcal{T}_i}(v) = 1$ and $v \neq R_i$. When this is the case, v necessarily has weight 1. This observation combined with (14.27) proves the claim (note that if $\deg_{\mathcal{T}_i}(R_i) > 1$, then, since $R_i \neq R$, we see that R_i must have degree at least 3 in $\mathcal{T}$, hence weight 2). $\square$

Returning to the proof of the proposition, note that the number of leaves of $\mathcal{T}$ which appear in some $\mathcal{T}_i$ is precisely the number of even-sized G_k-orbits of leaves of $\mathcal{T}$. Combining the claim with (14.26) thus gives

$$|\det M| = 2^{\#\{\text{even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\}} \cdot \prod_{i=1}^{s} \frac{d_{P(R_i)}}{2}. \tag{14.28}$$

For each $1 \leqslant i \leqslant s$, the parent of R_i lies in an odd sized G_k-orbit and has a child lying in an even-sized G_k-orbit. In particular, either $R_i = R$ or R_i has degree at least 3 in $\mathcal{T}$. Either way, $d_{R_i} = 2$ and the result follows. $\qquad\square$

In the remaining case, when $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of two principal clusters swapped by G_k, the result is the following.

Proposition 14.29. *Suppose that $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of two principal clusters $\mathfrak{s}_1$ and $\mathfrak{s}_2$ that are swapped by G_k. Then*

$$
|\det M| = \begin{cases} 2^{\#\{\text{even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\}} & g \text{ odd, or } g \text{ even and } \mathcal{R} \text{ not atypical,} \\ \frac{1}{2} \cdot 2^{\#\{\text{even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\}} & g \text{ even and } \mathcal{R} \text{ atypical.} \end{cases}
$$

Proof. We indicate how to adapt the proof of Proposition 14.21 to these cases.

Firstly suppose that g is odd. Then both $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are even. The vertices of $\mathcal{T}$ corresponding to $\Gamma_{\mathfrak{s}_1}$ and $\Gamma_{\mathfrak{s}_2}$ are joined by a path consisting of an odd number of vertices of multiplicity 2. Let R be the middle vertex in this path, which is fixed by G_k and has multiplicity 2. With this definition of R, the proof of Proposition 14.21 applies verbatim to give the desired result.

Now suppose that g is even, so that $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are both odd. Since $\mathfrak{s}_1$ and $\mathfrak{s}_2$ are swapped by G_k, we have $\delta_{\mathfrak{s}_1} = \delta_{\mathfrak{s}_2}$, and the vertices of $\mathcal{T}$ corresponding to $\Gamma_{\mathfrak{s}_1}$ and $\Gamma_{\mathfrak{s}_2}$ are joined by a path consisting of $\delta_{\mathfrak{s}_1}$ vertices of weight 1. If $\mathcal{R}$ is atypical, then this path consists of an odd number of vertices, and we take as a root R the middle vertex in this path. This is fixed by G_k and has weight 1. Following the proof of Proposition 14.21, (14.30) becomes

$$
|\det M| = 2^{\#\{\text{even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\}} \cdot \frac{d_R}{2}. \tag{14.30}
$$

To see this, note that every vertex of $\mathcal{T}$ other than R has an even-sized G_k-orbit, so that $s = 1$ in the proof of Proposition 14.21. The result now follows immediately.

Finally, suppose that g is even but that R is not atypical, so that the vertices of $\mathcal{T}$ corresponding to $\Gamma_{\mathfrak{s}_1}$ and $\Gamma_{\mathfrak{s}_2}$ are joined by a path consisting of a (positive since $\delta_{\mathfrak{s}_1} \geqslant 1$) even number of vertices. Let R_1 and R_2 be the middle vertices on this path, noting that they have degree 2 in $\mathcal{T}$ and weight 1. Note that every vertex of $\mathcal{T}$ has an even-sized G_k-orbit. As in the proof of Proposition 14.21, we compatibly pick a representative for each (even sized) G_k-orbit of vertices in $\mathcal{T}$, starting with R_1, and in such a way that if v is picked, then, for each G_k-orbit containing a child of v, the chosen representative of the orbit is itself a child of v. Let $\mathcal{T}_1$ be the subtree of $\mathcal{T}$ generated by the chosen vertices. This is a connected tree and we take R_1 as a root for $\mathcal{T}_1$. As in the proof of Proposition 14.21, define N_1 to be the matrix whose rows and columns are indexed by the vertices of $\mathcal{T}_1$ and such that the (v, v')-entry of N_1 is given by $(N_1)_{v,v'} = \frac{d_v d_{v'}}{r_v} \epsilon_v \cdot \epsilon_{v'}$. One then has $|\det M| = |\det N_1| \cdot \prod_{v \in \mathcal{T}_1} d_v^{-2}$. This time, the formula (14.25) is valid provided $(v, v') \neq (R_1, R_1)$. Noting that $\epsilon_{R_1} = R_1 - R_2$, one computes

$$
(N_1)_{R_1, R_1} = \frac{d_{R_1}^2}{2}(R_1 - R_2) \cdot (R_1 - R_2) = -2d_{R_1}^2 - \sum_{v \text{ child of } R_1 \text{ in } \mathcal{T}_1} m_v d_v d_{R_1}.
$$

Again, the matrix N_1 satisfies the conditions of Lemma 14.22, and the row corresponding to R_1 sums to $2d_{R_1}^2$. Thus,

$$|\det M| = 2 \cdot \prod_{v \in \mathcal{T}_1, \, v \neq R_1} \frac{d_{P(v)}}{d_v}.$$

Now $\mathcal{T}_1$ consists of at least two vertices, R_1 has degree 1 in $\mathcal{T}_1$ and weight 1 and leaves of $\mathcal{T}_1$ other than R_1 correspond bijectively to (necessarily even sized) G_k-orbits of leaves in $\mathcal{T}$, all of which have weight 1. Arguing as in the claim in the proof of Lemma 14.22 now gives the result. □

Recall from Notation 13.24 that we set $\kappa(C) = 1$ if $\mathcal{R} = \mathfrak{s}_1 \sqcup \mathfrak{s}_2$ is a disjoint union of two odd G_k-conjugate clusters with both δ_{s_1} and δ_{s_2} odd, and set $\kappa(C) = 0$ otherwise. Putting everything together, we obtain the following.

Corollary 14.31. *We have*

$$\epsilon(C^L/K) + \mathrm{ord}_2 c(J^L/K) \equiv \kappa(C) + \#\left\{\text{even-sized } G_k\text{-orbits on } \mathcal{R} \cap K^{\mathrm{nr}}\right\} +$$

$$\#\left\{G_k\text{-orbits } O \subseteq T \text{ with } \prod_{\mathfrak{t} \in O} \epsilon_\mathfrak{t}(F) \gamma_{\mathfrak{t}, L}(F) = -1\right\} \pmod 2.$$

Proof. Combining (14.20) with 14.21, 14.29 gives

$$\epsilon(C^L/K) + \mathrm{ord}_2 c(J^L/K) \equiv \kappa(C) + \#\{\text{even-sized } G_k\text{-orbits of leaves of } \mathcal{T}\} \pmod 2. \tag{14.32}$$

As in Remark 14.9, there are $2g + 2$ leaves of $\mathcal{T}$. By Remark 14.14, the leaves corresponding to elements $r \in \mathcal{R}$, together with leaves arising as the crosses on the crossed tails $T_\mathfrak{t}$ for twins $\mathfrak{t} \notin T$, form a G_k-set isomorphic to $\mathcal{R} \cap K^{\mathrm{nr}}$. These leaves give rise to the second term on the right-hand side of the statement. The remaining leaves arise as the crosses on the crossed tails $T_\mathfrak{t}$ corresponding to twins $\mathfrak{t} \in T$. Using Proposition 14.13, we see that each G_k-orbit $O \subseteq T$ gives rise to a single even sized G_k-orbit of leaves if $\prod_{\mathfrak{t} \in O} \epsilon_\mathfrak{t}(F) \gamma_{\mathfrak{t}, L}(F) = -1$, and either 0 or 2 such orbits if $\prod_{\mathfrak{t} \in O} \epsilon_\mathfrak{t}(F) \gamma_{\mathfrak{t}, L}(F) = 1$ (according to whether $|O|$ is odd or even). This gives the result. □

15 | PROOF OF PROPOSITION 11.1

For this section, we take K to be a non-archimedean local field of odd residue characteristic, take $L = K(\sqrt{\pi})$ to be a ramified quadratic extension of K and let C/K be a semistable hyperelliptic curve. We now combine the results of Sections 11–14 to prove Proposition 11.1. For convenience, we recall the statement.

Proposition 15.1 (=Proposition 11.1). *Conjecture 1.7 holds for C and L/K.*

Proof. By Lemma 4.1, we are at liberty to replace K with an arbitrarily large odd-degree unramified extension. In particular, we can without loss of generality assume that C/K is given by an equation of the form $y^2 = f(x)$ where $f(x)$ satisfies Assumption 13.4 (see Remark 13.5 for a

justification of this). This allows us to use the results of Sections 13.4 and 14 which were proven under this simplifying assumption.

Combining Corollary 13.25 and Corollary 14.31 with (11.2) and (11.8) gives

$$w(J/L) \cdot (-1)^{\varepsilon(C/K) + \varepsilon(C^L/K) + \dim J(K)/N_{L/K} J(L)} = (-1)^{\#\left\{\text{even-sized } G_k\text{-orbits on } \mathcal{R} \cap K^{\mathrm{nr}}\right\}}$$

$$\cdot (-1)^{\#\left\{G_k\text{-orbits } O \subseteq T \text{ with } \prod_{t \in O} \gamma_{t,L}(F) = -1\right\}}.$$

Here, we are using the notation of Sections 13, 14, so that $\mathcal{R}$ denotes the set of roots of $f(x)$ in K^s, the set T is as defined in Notation 13.8 and the signs $\gamma_{t,L}$ are as defined in Notation 14.12. To prove Conjecture 1.7, we see that it suffices to establish the equality

$$(\Delta_C, L/K) \overset{?}{=} (-1)^{\#\left\{\text{even-sized } G_k\text{-orbits on } \mathcal{R} \cap K^{\mathrm{nr}}\right\} + \#\left\{G_k\text{-orbits } O \subseteq T \text{ with } \prod_{t \in O} \gamma_{t,L}(F) = -1\right\}}. \tag{15.2}$$

Recall from Lemma 13.9 that we have $\cup_{t \in T} t = \mathcal{R} \setminus \mathcal{R} \cap K^{\mathrm{nr}}$, and that each $t = \{r_{t,1}, r_{t,2}\}$ is an inertia orbit of roots of $f(x)$. In particular, we can factor $f(x)$ over K as a product

$$f(x) = f_{\mathrm{nr}}(x) \cdot \prod_{O \in T/G_k} f_O(x)$$

where $f_{\mathrm{nr}}(x) \in K[x]$ splits over K^{nr} and where, for a G_k-orbit $O \subseteq T$, we have

$$f_O(x) = \prod_{t \in O} (x - r_{t,1})(x - r_{t,2}) \in K[x].$$

In what follows, for a polynomial $g(x)$, we write Δ_g for its discriminant. From the above factorisation, we find

$$(\Delta_C, L/K) = (\Delta_{f_{\mathrm{nr}}}, L/K) \cdot \prod_{O \in T/G_k} (\Delta_{f_O}, L/K).$$

This follows from the fact that, for coprime polynomials $h_1(x), h_2(x) \in K[x]$, we have $\Delta_{h_1 h_2} = \Delta_{h_1} \Delta_{h_2} \mathrm{Res}(h_1, h_2)^2$ where $\mathrm{Res}(h_1, h_2) \in K^\times$ denotes the resultant of $h_1(x)$ and $h_2(x)$.

Since L/K is ramified whilst $f_{\mathrm{nr}}(x)$ splits over an unramified extension, we see that $(\Delta_{f_{\mathrm{nr}}}, L/K) = 1$ if and only if $\Delta_{f_{\mathrm{nr}}}$ is a square in K, which, in turn, happens if and only if the Frobenius element $F \in G_k$ acts as an even permutation of the roots of $f_{\mathrm{nr}}(x)$. Thus, we have

$$(\Delta_{f_{\mathrm{nr}}}, L/K) = (-1)^{\#\left\{\text{even-sized } G_k\text{-orbits on } \mathcal{R} \cap K^{\mathrm{nr}}\right\}}.$$

To conclude, we claim that for each G_k-orbit $O \subseteq T$, we have $(\Delta_{f_O}, L/K) = \prod_{t \in O} \gamma_{t,L}(F)$. Indeed, from the definition of $\gamma_{t,L}$ given in Notation 14.12, we see that $\prod_{t \in O} \gamma_{t,L}(F)$ is equal to 1 if and only if the quantity

$$\prod_{t \in O} (r_{t,1} - r_{t,2})^2 (-\pi)^{-2d_t} \in \mathcal{O}_K^\times$$

is a square in K. We thus have

$$\prod_{\mathfrak{t}\in O} \gamma_{\mathfrak{t},L}(F) = \left(\prod_{\mathfrak{t}\in O} (r_{\mathfrak{t},1} - r_{\mathfrak{t},2})^2 (-\pi)^{-2d_{\mathfrak{t}}}, L/K \right) = \left(\prod_{\mathfrak{t}\in O} (r_{\mathfrak{t},1} - r_{\mathfrak{t},2})^2, L/K \right),$$

where for the second equality, we note that $-\pi$ is a norm from $L = K(\sqrt{\pi})$ (recall that, since $\mathfrak{t} \in T$, the quantity $2d_{\mathfrak{t}}$ is an odd integer). For $\mathfrak{t} \neq \mathfrak{t}' \in O$, write $R(\mathfrak{t}, \mathfrak{t}') = \prod_{r\in\mathfrak{t}, r'\in\mathfrak{t}'} (r - r')$, noting that this quantity lies in K^{nr} and that $R(\mathfrak{t}, \mathfrak{t}') = R(\mathfrak{t}', \mathfrak{t})$. Then, we have

$$\Delta_{f_O} = \prod_{\mathfrak{t}\in O} (r_{\mathfrak{t},1} - r_{\mathfrak{t},2})^2 \cdot \prod_{\{\mathfrak{t},\mathfrak{t}'\}\subseteq O} R(\mathfrak{t}, \mathfrak{t}')^2,$$

where the second product runs over all unordered pairs of distinct elements of O. The product $\prod_{\{\mathfrak{t},\mathfrak{t}'\}\subseteq O} R(\mathfrak{t}, \mathfrak{t}')$ is visibly fixed by G_K, and hence lies in K. We conclude that Δ_{f_O} and $\prod_{\mathfrak{t}\in O} (r_{\mathfrak{t},1} - r_{\mathfrak{t},2})^2$ are congruent modulo squares in $K^\times$, proving the claim. $\qquad\square$

16 | RESIDUE CHARACTERISTIC 2

In this section, we consider Conjecture 1.7 when K is a finite extension of $\mathbb{Q}_2$ and when the quadratic extension L/K is ramified. Let C/K be a hyperelliptic curve with Jacobian J. We suppose henceforth that J/K has good ordinary reduction. Let $J(K)_1$ denote the kernel of reduction on $J(K)$, and define $J(L)_1$ similarly. We begin by considering the norm map from $J(L)_1$ to $J(K)_1$.

Lemma 16.1. *We have*

$$\left| J(K)_1 / N_{L/K} J(L)_1 \right| = \left| J(K)_1[2] \right|.$$

Proof. Let $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$. Let g be the genus of C so that by [34, Theorem 1], there is a matrix $u \in \mathrm{Mat}_g(\mathbb{Z}_2)$ (the *twistmatrix* associated to the formal group of J) such that

$$J(K)_1 / N_{L/K} J(L)_1 \cong G^g / (1 - u) G^g.$$

Moreover, denoting by T the completion of K^{nr}, we have (see [34, Lemma])

$$J(K)_1 \cong \left\{ \alpha \in \left(\mathcal{O}_T^\times \right)^g : F\alpha = u\alpha \right\},$$

where F denotes the Frobenius automorphism of T. In particular, we have

$$J(K)_1[2] \cong \left\{ \alpha \in \{\pm 1\}^g : (1 - u)\alpha = 1 \right\}.$$

Identifying the groups G and $\{\pm 1\}$ in the obvious way, $J(K)_1[2]$ is identified with the kernel of multiplication by $1 - u$ on G^g. We now conclude by noting that the cokernel and kernel of an endomorphism of a finite abelian group have the same order. $\qquad\square$

Lemma 16.2. *Suppose that $K(J[2])/K$ has odd degree. Then we have*

$$\dim J(K)/N_{L/K}J(L) \equiv 0 \pmod 2.$$

Proof. Lemma 4.1 reduces to the case $K(J[2]) = K$. In this case, we claim that

$$\dim J(K)/N_{L/K}J(L) = 2g.$$

To see this, consider the commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & J(L)_1 & \longrightarrow & J(L) & \longrightarrow & \tilde{J}(k) & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle N_{L/K}} & & \downarrow{\scriptstyle 2} & & \\
0 & \longrightarrow & J(K)_1 & \longrightarrow & J(K) & \longrightarrow & \tilde{J}(k) & \longrightarrow & 0,
\end{array}
$$

where $\tilde{J}/k$ denotes the special fibre of the Néron model of J. The assumption that all 2-torsion is defined over K means that reduction to the special fibre is a surjection from $J(K)[2]$ to $\tilde{J}(k)[2]$. In particular, in the exact sequence arising from applying the snake lemma to the diagram above, the connecting homomorphism is trivial. Thus, the sequence

$$0 \longrightarrow J(K)_1/N_{L/K}J(L)_1 \longrightarrow J(K)/N_{L/K}J(L) \longrightarrow \tilde{J}(k)/2\tilde{J}(k) \longrightarrow 0$$

is short exact. As J is ordinary (and all its 2-torsion is defined over K), we have

$$\left|\tilde{J}(k)/2\tilde{J}(k)\right| = \left|\tilde{J}(k)[2]\right| = 2^g.$$

On the other hand, by Lemma 16.1, we have

$$\left|J(K)/N_{L/K}J(L)\right| = \left|J(K)_1[2]\right| = 2^g$$

also, from which the result follows. $\qquad\square$

Corollary 16.3. *Suppose that $K(J[2])/K$ has odd degree. Then Conjecture 1.7 holds for C/K and the extension L/K.*

Proof. Again by Lemma 4.1, we can assume that all the 2-torsion of J is defined over K. Under this assumption, $f(x)$ splits over K, so $(\Delta_C, L/K) = 1$. Similarly, both C and C^L have a K-rational Weierstrass point, so $\epsilon(C/K) + \epsilon(C^L/K) = 0$. By Lemma 16.2, we have $(-1)^{\dim J(K)/N_{L/K}J(L)} = 1$, and, for example, by [15, Proposition 3.23], we have $w(J/L) = 1$. $\qquad\square$

For the purpose of giving examples, we now describe how to construct hyperelliptic curves over $\mathbb{Q}$ whose Jacobians are good ordinary over $\mathbb{Q}_2$ and have all their 2-torsion defined over an odd degree extension on $\mathbb{Q}_2$. Let $g \geqslant 2$ be an integer.

Lemma 16.4. *Let $f(x) \in \bar{\mathbb{F}}_2[x]$ be a monic separable polynomial of degree $g + 1$ and let $h(x) \in \bar{\mathbb{F}}_2[x]$ be a polynomial of degree $\leqslant g$, coprime to $f(x)$. Then the hyperelliptic curve*

$$C/\bar{\mathbb{F}}_2 : y^2 - f(x)y = h(x)f(x)$$

is ordinary.

Proof. One readily checks that the equation defining C is smooth, and hence defines a hyperelliptic curve over $\bar{\mathbb{F}}_2$ of genus g. Let J be the Jacobian of C. As in the proof of [14, Theorem 23], one sees that $\dim J(\bar{\mathbb{F}}_2)[2] = g$, and hence J is ordinary. □

Lemma 16.5. *Suppose $f(x) \in \mathbb{Z}[x]$ has odd leading coefficient and degree $g + 1$, and suppose that $f(x)$ (mod 2) is separable with each irreducible factor having odd degree. Further, let $h(x) \in \mathbb{Z}[x]$ have degree $\leqslant g$ be such that $h(x)$ (mod 2) is coprime to $f(x)$ (mod 2). Then the Jacobian J of the hyperelliptic curve*

$$C : y^2 = f(x)(f(x) + 4h(x))$$

has good ordinary reduction over $\mathbb{Q}_2$. Moreover, $\mathbb{Q}_2(J[2])/\mathbb{Q}_2$ has odd degree.

Proof. A change of variables over $\mathbb{Q}_2$ brings C into the form $y^2 - f(x)y = h(x)f(x)$, so J has good ordinary reduction over $\mathbb{Q}_2$ by Lemma 16.4. Moreover, both $f(x)$ and $f(x) + 4h(x)$ reduce to separable polynomials over $\mathbb{F}_2$ whose irreducible factors have odd degree. It follows from Hensel's lemma that $f(x)(f(x) + 4h(x))$ splits over an odd degree unramified extension of $\mathbb{Q}_2$, and hence $\mathbb{Q}_2(J[2])/\mathbb{Q}_2$ has odd degree (and is unramified). □

17 | **PROOF OF THEOREMS 1.1 AND 1.8**

We have now established enough cases of Conjecture 1.7 to deduce 1.1, 1.8. For completeness, we explain these deductions below.

Proof of Theorem 1.8. The case where K is non-archimedean is Proposition 7.1. The case where the quadratic extension is unramified is Proposition 9.1. For the remaining cases, combine Proposition 11.1 (=Proposition 15.1) and Proposition 16.3. These deal, respectively, with ramified extensions in odd residue characteristic, and ramified extensions in residue characteristic 2. □

Proof of Theorem 1.1. As explained in Section 1.3, this follows by combining Theorem 1.6 (=Theorem 2.1) with Theorem 1.8. □

Compared to [40], the main results are strengthened by drawing on the works [18] and [20], and I am grateful to Omri Farragi and Sarah Nowell for answering my questions about their work [20]. I would also like to thank Alex Bartel, L. Alexander Betts, Vladimir Dokchitser, Qing Liu and Céline Maistret for helpful conversations, and a referee for carefully reading the paper and suggesting several improvements.

DATA AVAILABILITY STATEMENT

Not applicable.

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.

ORCID

Adam Morgan https://orcid.org/0000-0003-2824-9070

REFERENCES

1. M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory Proc. Instructional Conf., Brighton, 1965, pp. 94–115.
2. A. J. Best, L. A. Betts, M. Bisatt, R. van Bommel, V. Dokchitser, O. Faraggi, S. Kunzweiler, C. Maistret, A. Morgan, S. Muselli, and S. Nowell, *A user's guide to the local arithmetic of hyperelliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 3, 825–867.
3. L. A. Betts, *Variation of Tamagawa numbers of Jacobians of hyperelliptic curves with semistable reduction*, J. Number Theory **231** (2022), 158–213.
4. L. 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. With an appendix by V. Dokchitser and A. Morgan.
5. S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math. **98** (1999), no. 3, 275–293.
6. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Erg. Math., vol. 21, Springer, Berlin, 1990.
7. J. W. S. Cassels, *Global fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 42–84.
8. K. Česnavičius, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math. **719** (2016), 45–73.
9. K. Česnavičius, *The ℓ-parity conjecture over the constant quadratic extension*, Math. Proc. Cambridge Philos. Soc. **165** (2018), no. 3, 385–409.
10. K. Česnavičius and N. Imai, *The remaining cases of the Kramer-Tunnell conjecture*, Compos. Math. **152** (2016), no. 11, 2255–2268.
11. J. Coates, T. Fukaya, K. Kato, and R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), 19–97.
12. G. Cornelissen, *Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. (Basel) **77** (2001), no. 3, 241–246.

13. G. Cornelissen, *Erratum to: Two-torsion in the Jacobian of hyperelliptic curves over finite fields*, Arch. Math. (Basel) **85** (2005), no. 6, loose erratum.

14. W. Castryck, M. Streng, and D. Testa, *Curves in characteristic 2 with non-trivial 2-torsion*, Adv. Math. Commun. **8** (2014), no. 4, 479–495.

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

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

17. T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **658** (2011), 39–64.

18. T. Dokchitser, V. Dokchitser, C. Maistret, and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. (2023), 1213–1322.

19. V. Dokchitser and C. Maistret, *On the parity conjecture for abelian surfaces*, Proc. London Math. Soc. **127** (2023), no. 2, 295–365.

20. O. Faraggi and S. Nowell, *Models of hyperelliptic curves with tame potentially semistable reduction*, Trans. London Math. Soc. **7** (2020), no. 1, 49–95.

21. J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), no. 3, 515–538.

22. H. Green and C. Maistret, *2-parity conjecture for elliptic curves with isomorphic 2-torsion*, Proc. R. Soc. A. **478** (2022), 20220012.

23. A. Grothendieck, *Modèles de Néron et monodromie*, SGA7-I, Expose IX, LNM 288, Springer, Berlin, 1972.

24. K. Gruenberg, *Profinite groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), 1967, pp. 116–127.

25. Z. Klagsbrun, B. Mazur, and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320.

26. K. Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135.

27. K. Kramer and J. Tunnell, *Elliptic curves and local ε-factors*, Compositio Math. **46** (1982), no. 3, 307–352.

28. S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136.

29. Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

30. Q. Liu, *Conducteur et discriminant minimal de courbes de genre 2*, Compositio Math. **94** (1994), no. 1, 51–79.

31. Q. Liu, *Modèles minimaux des courbes de genre deux*, J. Reine Angew. Math. **453** (1994), 137–164.

32. Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610.

33. D. Lorenzini, *Torsion and Tamagawa numbers*, Ann. Inst. Fourier (Grenoble) **61** (2011), no. 5, 1995–2037.

34. J. Lubin and M. I. Rosen, *The norm map for ordinary abelian varieties*, J. Algebra **52** (1978), no. 1, 236–240.

35. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

36. B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.

37. B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, J. Algebra **314** (2007), no. 1, 419–438.

38. J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

39. J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

40. A. Morgan, *2-Selmer parity for Jacobians of hyperelliptic curves in quadratic extensions*, Ph.D. thesis, University of Bristol, 2015.

41. A. Morgan, *Quadratic twists of abelian varieties and disparity in Selmer ranks*, Algebra Number Theory **13** (2019), no. 4, 839–899.

42. D. Mumford, *Theta characteristics of an algebraic curve*, Ann. Sci. de l'École Norm. Sup. **4** (1971), 181–192.

43. Y. Namikawa and K. Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscripta Math. **9** (1973), 143–186.

44. J. Nekovář, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra Number Theory **7** (2013), no. 5, 1101–1120.

45. S. Nowell, *Models of hyperelliptic curves over p-adic fields*, Ph.D. thesis, University College London, 2022.

46. A. Obus and P. Srinivasan, *Conductor-discriminant inequality for hyperelliptic curves in odd residue characteristic*, IMRN (2023), to appear.

47. A. P. Ogg, *On pencils of curves of genus two*, Topology **5** (1966), 355–362.

48. B. Poonen and E. Rains, *Self cup products and the theta characteristic torsor*, Math. Res. Lett. **18** (2011), no. 6, 1305–1318.

49. B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269.

50. B. Poonen and E. F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188.

51. B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149.

52. M. Raynaud, *Variétés abéliennes et géométrie rigide*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, 1971, pp. 473–477.

53. I. Reiner, *The Schur index in the theory of group representations*, Michigan Math. J. **8** (1961), 39–47.

54. M. Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. **359** (2007), no. 9, 4259–4284.

55. M. Sadek, *On quadratic twists of hyperelliptic curves*, Rocky Mountain J. Math. **44** (2014), no. 3, 1015–1026.

56. E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114.

57. J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer, New York-Berlin, 1979. Translated from the French by M. J. Greenberg.

58. P. Srinivasan, *Invariants linked to models of curves over discrete valuation rings*, Ph.D. thesis, Massachusetts Institute of Technology, 2016.

59. P. Srinivasan, *Conductors and minimal discriminants of hyperelliptic curves: a comparison in the tame case*, arxiv:1910.08228, 2019.