# WILD CONDUCTOR EXPONENTS OF CURVES

HARRY SPENCER

Abstract. We give an explicit formula for wild conductor exponents of plane curves over $\mathbb{Q}_p$ in terms of standard invariants of explicit extensions of $\mathbb{Q}_p$, generalising a formula for hyperelliptic curves. To do so, we prove a general result relating the wild conductor exponent of a simply branched cover of the projective line with its associated discriminant cover. In an appendix we resolve a minor issue in the literature on the 3-torsion of genus 2 curves.

Contents



**Mathematics Subject Classification: 11G20, 11G10, 14H30, 11G40**

## 1. Introduction

Associated to a curve $C$ over a finite extension $K$ of $\mathbb{Q}_p$, is a representation-theoretic invariant which measures bad reduction called the *(local) conductor*. The conductor is an ideal $N = (\pi^{n_C})$, where $\pi$ is a uniformiser, and $n_C$ is the *conductor exponent*. In turn, $n_C$ is defined to be

$$n_C = n_{C,\text{tame}} + n_{C,\text{wild}},$$

where the *tame conductor exponent*, $n_{C,\text{tame}}$, can be extracted from a regular model of $C/K$. The *wild conductor exponent* is, in general, difficult to deal with but is 0 if $p > 2g_C + 1$, where $g_C$ is the genus of $C$. It is derived from the Galois-module (in fact, wild inertia-module) structure of the $\ell$-torsion $J_C[l]$ on the Jacobian of $C/K$ for any $p \neq \ell$. See §3.1 for the key points.

The problem of provably (and efficiently) finding conductors of elliptic curves is solved by Tate's algorithm, see [19, Chapter 4]. For hyperelliptic curves the problem is solved for $p \neq 2$ by means of an explicit formula in [6, Theorem 11.3]. In [13] the problem is solved for $p \neq 2$ for curves of genus at most 5. In [7, §4], by providing an algorithm for the explicit computation of 3-torsion (cf. §A), the problem is solved for genus 2 curves, and in [14, §3] the problem is solved for hyperelliptic genus 3 curves analogously. The problem is solved for plane quartics with a rational point in [15, Theorem 2]. A formula is given in [11, Theorem 4.1.4] for conductor exponents of superelliptic curves of exponent $n$, for $p \nmid n$.

In this work we show how wild conductor exponents can be determined from the ramification locus of a degree $n$ cover of $\mathbb{P}^1$, for $p > n$. We first treat the case of simply branched covers of $\mathbb{P}^1$.

**Theorem 1.1.** *Let $C/K$ be a curve over a finite extension of $\mathbb{Q}_p$ equipped with a simply branched degree $n$ cover of $\mathbb{P}^1$, with $p > n$. Any hyperelliptic curve $D$ whose degree 2 map to $\mathbb{P}^1$ has the same branch locus as this cover satisfies*

$$n_{C,\text{wild}} = n_{D,\text{wild}}.$$

**Remark 1.2.** Every such curve $C/K$ admits a simply branched cover of degree at most $g_C+1$ (possibly after base change to a tame extension of $K$), cf. Remark 5.11. ♢

In fact, we prove a stronger result (Theorem 5.2) which replaces $\mathbb{P}^1$ by an arbitrary curve $B$, replaces the hyperelliptic curve by a degree 2 cover of $B$, has an additional summand of $(n-1)\cdot n_{B,\text{wild}}$, allowing a slightly weaker restriction on ramification.

By appealing to [6, Theorem 11.3] (cf. Theorem 6.1), which gives an explicit formula for wild conductor exponents of hyperelliptic curves over finite extensions of $\mathbb{Q}_p$, $p \neq 2$, we obtain an analogous formula for some plane curves. In fact, [6, Theorem 11.3] is the special case $n = 2$ of the following theorem, for which we first introduce some important notation.

**Notation.** For $K$ a finite extension of $\mathbb{Q}_p$ and a polynomial $g \in K[t]$ write

$$w_K(g) = \sum_{r \in R/G_K} m(r) \cdot (v_K(\Delta_{K(r)/K}) - [K(r) : K] + f_{K(r)/K}),$$

where $R$ denotes the set of $\overline{K}$-roots of $g$, $\Delta_\bullet$ the discriminant, $f_\bullet$ the residue degree, and $m(\bullet)$ the multiplicity of a root.

**Remark 1.3.** When $g$ is square-free, $w_K(g)$ is the wild conductor exponent of the hyperelliptic curve $y^2 = g(t)$ if $p \neq 2$. Therefore the computation of $w_K(g)$ for general $g$ is essentially already implemented, e.g. in Magma [3]. ♢

**Theorem 1.4** (=Theorem 6.5)**.** *Let $\mathcal{C} : f(x, y) = 0$ be a smooth affine curve over a finite extension $K$ of $\mathbb{Q}_p$ with smooth normalisation $C$. If $p > \deg_x f$, then*

$$n_{C,\text{wild}} = w_K(\operatorname{disc}_x f).$$

**Remark 1.5.** To prove Theorem 1.4 we need Theorem 5.2, which allows one branch point above which our cover as in Theorem 1.1 is not simply branched, assuming that we have $S_n$-Galois closure. Note that a simply branched cover of $\mathbb{P}^1$ of degree $n$ must have $S_n$-Galois closure (cf. [2, Corollary 3.2]), and usually so do curves satisfying this less strict criterion. ♢

**Remark 1.6.** Given a curve $C$ embedded smoothly in $\mathbb{P}^n$ equipped with a cover $\pi : C \to \mathbb{P}^1$, one could obtain a similar result to Theorem 1.4, replacing $\operatorname{disc}_x f$ by

$$\prod_{t \in \mathbb{P}^1} \prod_{P \in \pi^{-1}(t)} (x - t)^{e_P - 1},$$

where $e_P$ denotes the ramification index at $P$, provided that one can perturb the defining equations of $C$ to obtain simply branched covers $\widetilde{\pi} : \widetilde{C} \to \mathbb{P}^1$. ♢

For example, Theorem 1.4 gives a simple formula for the wild conductor exponent of some superelliptic curves of exponent $n$ for $p > n$.

**Corollary 1.7** (=Corollary 6.6)**.** *Consider a superelliptic curve $C/K : y^n = f(x)$, $f$ square-free, over a finite extension $K$ of $\mathbb{Q}_p$. If $p > n$, then*

$$n_{C,\text{wild}} = (n-1) \cdot w_K(f).$$

All we are using here about these curves is that they are obviously smooth on this affine chart. In particular, we do not use any of the additional structure afforded to a superelliptic curve by nature of it being a cyclic cover of $\mathbb{P}^1$—in fact, using perturbations, we deliberately rid ourselves of this structure. In forthcoming work of Obus and Srinivasan, this structure is harnessed using different techniques to generalise Corollary 6.6:

**Proposition 1.8.** *Consider a superelliptic curve $C/K : y^n = f(x)$ over a finite extension $K$ of $\mathbb{Q}_p$. Suppose $f = \prod_{i=1}^r f_i^{d_i}$ with the $f_i$ being distinct irreducible polynomials, each $d_i$ satisfying $1 \leq d_i \leq n-1$, and $\gcd(n, d_1, \ldots, d_r) = 1$. If $p \nmid 2n$, then*

$$n_{C,\text{wild}} = \sum_{i=1}^{r} (n - \gcd(n, d_i)) \cdot w_K(f_i).$$

In Remark 4.3 we give a brief discussion of how the same result could be obtained from the techniques herein.

We can also apply Theorem 1.4 in vastly more general settings; the following example computes the wild conductor exponent of a non-superelliptic curve over $\mathbb{Q}_7$, using Magma for the numerical computations.

**Example 1.9.** Consider the curve $C/\mathbb{Q}_7 : f(x,y) = 7x^3y^4 + x + y^5 + 7 = 0$ of genus 6. We compute that

$$n_{C,\text{wild}} = w_{\mathbb{Q}_7}(-1323y^{18} - 18522y^{13} - 64827y^8 - 28y^4) = 14.$$

As a sanity check, one can also compute

$$n_{C,\text{wild}} = w_{\mathbb{Q}_7}(\operatorname{disc}_y f) = 14,$$

verifying the (*a priori* non-obvious) fact that the quantity $w_K(\operatorname{disc}_x f)$ is independent of the labelling of $x$ and $y$, provided that the residue characteristic is greater than $\max\{\deg_x f, \deg_y f\}$. ♢

We use the framework of *motivic pieces of curves* set out in [8, §2], the key parts of which we recall in §3.4. For a curve $X$ admitting an action by automorphisms of the finite group $G$ and a $G$-representation $\rho$, define

$$X^\rho = \operatorname{Hom}_G(\rho, (V_\ell J_X)^*).$$

In §4 we obtain relations between the conductors of these representations for curves with a cyclic action.

**Proposition 1.10** (=Proposition 4.4)**.** *Let $K$ be a finite extension of $\mathbb{Q}_p$. Given a $C_n$-cover $\pi : X \to B$, write $R_q$ for the number of points with ramification index divisible by $q$ for each $q \mid n$ prime. For $p > \max_{q|n}\{q, (R_q - 2)(q-1) + 1\}$, for any irreducible representation $\rho$ of $C_n$ we have*

$$n_{\text{wild}}(X^\rho) = n_{\text{wild}}(X^{\mathbb{1}}).$$

In §5, using an Artin-like induction lemma, we piece together these cyclic relations, establishing Theorem 5.2 and hence Theorem 1.1. Theorem 1.4 will follow from Theorem 5.2 by combining the following local constancy result with the local constancy of wild conductor exponents (e.g. [10, Theorem 5.1(1)]).

**Lemma 1.11** (=Lemma 6.3)**.** *Let $K/\mathbb{Q}_p$ be a finite extension. Let $g \in K[t]$ be $p^{th}$-power-free and suppose square-free $h \in K[t]$ is sufficiently close to $g$. We have $w_K(h) = w_K(g)$.*

We have numerically tested Theorem 1.4 against known conductor exponents of curves. When testing against [7, Proposition 4.1], which is used to compute wild conductor exponents at $p = 2$ of genus 2 curves, we discovered a minor error in the latter. Therefore, lastly, in Appendix A we fix this error.

**Conventions.** Throughout, a curve over $k$ is taken to be a geometrically connected, smooth, projective $k$-variety of dimension 1. We use the correspondence between finitely generated transcendence degree 1 extensions of a field $k$ and normal curves over $k$, and in particular—outside of §6—we are referring to the unique normalisation of the projective closure whenever we describe a curve by a possibly-singular affine model. We take $\mathbb{P}^1$ to mean a genus 0 curve with a rational point and hyperelliptic curves to be double covers of $\mathbb{P}^1$.

Acknowledgements

My utmost gratitude goes to Vladimir Dokchitser for his wise supervision, without which this work would not have been possible. I thank Alexandros Konstantinou for his additional guidance and many fruitful discussions, Elvira Lupoian for helpful comments on a draft, James Rawson for helpful correspondence regarding Remark 5.11, Tim Dokchitser for helpful correspondence regarding Appendix A, and Andrew Obus and Padmavathi Srinivasan for sharing their work on Proposition 1.8. Lastly, I thank the anonymous referee for their suggestions towards improving the clarity of the arguments herein.

This work was supported by the Engineering and Physical Sciences Research Council [EP/S021590/1], the EPSRC Centre for Doctoral Training in Geometry and Number Theory (The London School of Geometry and Number Theory), University College, London.

## 2. Notation

| Notation | Terminology |
|---|---|
| $W_K \leq G_K$ | Absolute Galois group and wild inertia subgroup |
| $v_K$ | Normalised valuation on $p$-adic field $K$ |
| $e_{K'/K}$, $f_{K'/K}$ | Ramification and inertia degrees of extension of $p$-adic fields |
| $g_X$ | Genus of a curve $X$ |
| $J_X$ | Jacobian variety associated to a curve $X$ |
| $X/H$ | Quotient curve by the action of a finite group $H$ |
| $T_\ell A$, $V_\ell A$ | $\ell$-adic Tate module of an abelian variety, $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ |
| $C_n$ | Cyclic group of order $n$ |
| $S_n$ | Symmetric group on $n$ letters |
| $F_n$ | Standard irreducible $S_n$-representation (cf. Definition 5.1) |
| $S_{n-1}^\circ$ | Subgroup stabilising a point under $S_n$-action on $n$ letters |
| $\langle , \rangle$ | Representation-theoretic inner product on characters |
| $\mathrm{Ind}_H^G \chi$ | Induction of a character $\chi$ of $H \leq G$ to $G$ |
| $\mathrm{Res}_H \chi$ | Restriction of a character $\chi$ of $G$ to $H \leq G$ |
| $\mathbb{Q}(\chi)$ | Field generated by $\{\chi(g)\}_{g \in G}$ for a character $\chi$ of $G$ |

## 3. Background

3.1. **Wild conductor exponents.** We fix a finite extension $K$ of $\mathbb{Q}_p$ and consider an $G_K$-representation $V$ over either $\mathbb{Q}_l$ or $\mathbb{F}_l$, where $\ell \neq p$.

**Definition 3.1** (e.g. [20, pages 3–4])**.** The *wild conductor exponent* of $V$ is

$$n_{\text{wild}}(V) = \int_0^\infty \operatorname{codim}(V^{G_K^u})\mathrm{d}u,$$

where the $G_K^u$ are higher ramification groups in upper numbering.

In particular, $n_{\text{wild}}(V)$ is determined only by the action of wild inertia. In fact, in the case of curves, the wild conductor exponent depends only on the action of wild inertia on $\ell$-torsion for any $\ell \neq p$.

Serre and Tate showed that the wild conductor exponents attached to abelian varieties vanish for $p$ sufficiently large relative to the dimension.

**Proposition 3.2.** *Let $A$ be an abelian variety of dimension $g$ over a finite extension of $\mathbb{Q}_p$. If $p > 2g+1$, then $n_{\text{wild}}(V_\ell A) = 0$ for all $\ell \neq p$.*

*Proof.* See the proof of [18, Corollary 2]. □

We will make use of the following similar constraint.

**Lemma 3.3.** *Let $K$ be a finite extension of $\mathbb{Q}_p$ and fix a prime $\ell \neq p$. Suppose there are abelian varieties $A_1, \dots, A_n$ and $B_1, \dots, B_m$ and some wild inertia representation $W$ of dimension $2d$ over $\mathbb{F}_\ell$ such that*

$$W \oplus \bigoplus_i A_i[\ell] \cong \bigoplus_j B_j[\ell]$$

*as wild inertia representations. If $p > 2d+1$, then $n_{\text{wild}}(W) = 0$.*

*Proof.* Suppose $p > 2d+1$ and consider a wild inertia element $\sigma$ acting non-trivially on $\bigoplus_j B_j[\ell]$ as an element of order $p^r$. The characteristic polynomial of $\sigma$ has integer coefficients, e.g. by the well-known independence of $\ell$ of Weil–Deligne representations associated to abelian varieties.

Therefore each primitive root of unity appears as an eigenvalue of $\sigma$ on $W \oplus \bigoplus_i A_i[\ell]$ with equal multiplicity. The same is true for each $A_i[\ell]$, so each root of unity must appear as an eigenvalue of $\sigma$ acting on $W$. There must be at least $p-1 > 2d$ such eigenvectors, which is not possible, so the action on $W$ is trivial. □

Lastly, we note that one can keep track of wild conductor exponents under tamely ramified base change.

**Lemma 3.4.** *Let $V$ be an $\ell$-adic representation over a finite extension $K$ of $\mathbb{Q}_p$. Suppose $K'/K$ is a tamely ramified extension. We have*

$$n_{\text{wild}}(\operatorname{Res}_{G_{K'}} V) = e_{K'/K} \cdot n_{\text{wild}}(V).$$

*Proof.* This follows from the fact that $G_K^u \cap G_{K'} = G_{K'}^{ue_{K'/K}}$. □

3.2. **Galois covers and Galois closure.** Recall that a cover of curves is a surjective morphism $\pi : X \to B$ of curves over a field $K$. Functorially, we obtain an embedding of function fields $K(B) \hookrightarrow K(X)$.

**Definition 3.5.** We say $\pi$ is a *Galois cover* if $K(X)/K(B)$ is a Galois extension, and we will say $\pi$ is a $G$-cover if $\pi$ is Galois, $\operatorname{Gal}(K(X)/K(B)) \cong G$ and $K(X)$ contains no algebraic extension of $K$.

Given a non-Galois cover $\pi : X \to B$, we say the *Galois closure* is the curve whose function field is the Galois closure of the extension $K(X)/K(B)$. We say that a cover has $G$-Galois closure if its Galois closure is a $G$-cover.

We will often write 'cyclic cover', 'symmetric cover' etc. to mean a Galois cover of curves whose Galois group has this property.

We will be particularly interested in the ramification properties of covers and especially in the case where covers are simply branched.

**Definition 3.6.** A degree $n$ cover of curves $\pi : X \to B$ is *simply branched* if for each $P \in B$ we have $|\pi^{-1}(P)| \geq n - 1$.

Alternatively, consider the Galois closure $\widetilde{\pi} : \widetilde{X} \to B$ of $\pi : X \to B$, writing $G = \mathrm{Gal}(\pi)$ and take $H \leq G$ such that $X = \widetilde{X}/H$. Then $\pi$ is simply branched if the decomposition group of $\mathfrak{P} \in \widetilde{X}$ above $P \in B$ acts either trivially or by a single transposition on $G/H$.

3.3. **Kernels of pull-backs and push-forwards.** Given a cover of curves $\pi : X \to B$, we define the Prym variety associated to $\pi$ to be the connected component of $\ker(\pi_* : J_X \to J_B)$ containing the identity, denoted $\mathrm{Prym}(\pi)$. The following well-known proposition governs the index of $\mathrm{Prym}(\pi)$ in $\ker \pi_*$ and, dually, the kernel of the pull-back $\pi^* : J_B \to J_X$.

**Proposition 3.7.** *Let $p$ be a prime and $\pi : X \to B$ a $C_p$-cover of curves over a field $K$ of characteristic different from $p$. Either*

*(1) $\pi$ is unramified, $\ker(\pi_*)/\mathrm{Prym}(\pi) \cong \langle T \rangle$ for some $T \in J_X[p]$ and $\ker \pi^* = \langle P \rangle$ for some $P \in J_B[p]$, or*
*(2) $\pi$ is ramified, $\ker \pi_*/\mathrm{Prym}(\pi) = 1$ and $\pi^*$ is injective.*

*Proof.* For (1): see the main theorem of [16] for the claim about $\ker \pi_*$ and [1, Lemma 2.2] for the claim about $\ker \pi^*$.

For (2): we will show that $\pi^*$ is injective; the claim about $\ker \pi_*$ is equivalent by Cartier duality, e.g. as shown in [5, proof of Proposition 3.3].

Because $\pi_* \pi^* = [p]$, we have $\ker \pi^* \subseteq J_B[p]$. Now, subgroups generated by points $0 \neq P \in J_B[p]$ correspond by Kummer theory to unramified $C_p$-covers $B_P \to B$ over $\overline{K}$, or equivalently to unramified $C_p$-extensions $\overline{K}(B_P)/\overline{K}(B)$. In terms of function fields, the pull-back $\pi^*(P)$ corresponds to the extension $\overline{K}(X)\overline{K}(B_P)/\overline{K}(X)$, which is an unramified $C_p$-extension of $\overline{K}(X)$. The existence of $P \in \ker \pi^*$ would say $\overline{K}(X)\overline{K}(B_P) = \overline{K}(X)$, a contradiction. □

3.4. **Motivic pieces of curves.** We summarise the key definition and some basic properties from [8, §2]. Fix a $G$-cover of curves $\pi : X \to B$ over $K$.

Consider the action (inherited from that on the points of $X$) of $G$ on $V_\ell J_X$, noting that this commutes with the action of $G_K$ because our cover is $K$-rational.

**Definition 3.8** (=[8, Definition 2.3])**.** For a $G$-representation $\rho$, define

$$X^\rho = \mathrm{Hom}_G(\rho, (V_\ell J_X)^*),$$

on which $G_K$ acts by postcomposition. Implicitly this requires a choice of $\ell$, but the usual independence properties hold (cf. [8, Corollary 2.14]).

Recall that a virtual character is a $\mathbb{Z}$-linear combination of characters.

**Definition 3.9.** For a virtual character $\chi = \sum_i r_i \rho_i$ of $G$, we define

$$n_{\mathrm{wild}}(X^\chi) = \sum_i r_i \cdot n_{\mathrm{wild}}(X^{\rho_i}).$$

Note that Galois-conjugate pieces will have the same wild conductor exponents:

**Lemma 3.10.** *Let $X$, $G$ and $\rho$ be as above. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})$, we have*

$$n_{\mathrm{wild}}(X^{\rho}) = n_{\mathrm{wild}}(X^{\sigma(\rho)}).$$

*Proof.* Choosing $\ell$ prime to $p$, [8, Lemma 2.12] implies that

$$\mathrm{Tr}(\alpha | H^1_\ell(X^\rho))^\sigma = \mathrm{Tr}(\alpha | H^1_\ell(X^{\sigma(\rho)}))$$

for $\alpha \in W_K$. Wild inertia acts through a finite quotient, say $W$, so we have that $H^1_\ell(C^\tau)$ and $H^1_\ell(C^{\sigma(\tau)})$ are conjugate $W$-representations. That the wild conductor exponents are equal follows. □

The following key properties come from an analogue of the 'Artin formalism'.

**Lemma 3.11.** *Fix $X$, $B$ and $G$ as above and take $K$ to be a finite extension of $\mathbb{Q}_p$. For $\rho_1$ and $\rho_2$ two representations of $G$, and $\tau$ a representation of $H \leq G$:*

*(1)* $n_{\mathrm{wild}}(X^{\rho_1+\rho_2}) = n_{\mathrm{wild}}(X^{\rho_1}) + n_{\mathrm{wild}}(X^{\rho_2})$

*(2)* $n_{\mathrm{wild}}(X^{\mathrm{Ind}_H^G \tau}) = n_{\mathrm{wild}}(X^{\tau})$.

*Proof.* Follows from [8, Proposition 2.8]. □

A special case of Lemma 3.11 is the following observation, which shows how we translate between wild conductor exponents of curves and of motivic pieces.

**Lemma 3.12.** *For $H \leq G$, we have*

$$n_{X/H,\mathrm{wild}} = n_{\mathrm{wild}}(X^{\mathrm{Ind}_H^G \mathbb{1}}).$$

**Notation.** We write $S_{n-1}^{\circ}$ for the subgroup of $S_n$ which stabilises $n$.

**Example 3.13.** Consider an $S_n$-cover $X \to B$. Let $F$ be the standard irreducible representation of $S_n$ (cf. Definition 5.1). We have

$$n_{X/S_{n-1}^{\circ},\mathrm{wild}} = n_{\mathrm{wild}}(X^{F+\mathbb{1}}). \qquad \diamondsuit$$

## 4. Cyclic covers

In this section, given a cyclic cover of curves $X \to B$, we establish relations between wild conductor exponents of $X$ and $B$. We first treat the case of cyclic covers of prime order, before moving onto general cyclic groups.

### 4.1. Cyclic groups of prime order.

The first case we treat is that of $C_2$-covers of curves.

**Proposition 4.1.** *Suppose $\pi : X \to B$ is an $C_2$-cover of curves over a finite extension of $\mathbb{Q}_p$, ramified at $R$ points. For $p > \max\{3, R\}$, we have*

$$n_{X,\mathrm{wild}} = 2 \cdot n_{B,\mathrm{wild}}.$$

*Equivalently, for $\varepsilon$ the non-trivial irreducible representation of $C_2$, we have*

$$n_{\mathrm{wild}}(X^{\varepsilon}) = n_{\mathrm{wild}}(X^{\mathbb{1}}).$$

*Proof.* In the unramified case, the map $\pi_* : J_X[2] \to J_B[2]$ has cokernel of size 2 by Proposition 3.7, which says that the image has size $2^{2g_X-(2g_X-2g_B+1)} = 2^{2g_B-1}$, and $\pi^*$ is injective.

We can apply Maschke's Theorem (e.g. [17, Theorem 1]) because wild inertia acts through a quotient of $p$-power order, and so by a group of order prime to 2, so we have some one-dimensional wild inertia representation $V$ such that $J_X[2] \oplus V \cong J_B[2] \oplus \ker \pi_*[2]$.

Also, $\pi^* J_B[2] \leq \ker \pi_*[2]$ and counting gives an equality. Applying Maschke's Theorem to $\ker \pi^* \leq J_B[2]$, there is another one-dimensional wild inertia representation $V'$ such that $J_B[2] \cong \pi^* J_B[2] \oplus V'$, so $J_X[2] \oplus V' \oplus V \cong J_B[2] \oplus J_B[2]$. We have $n_{\text{wild}}(V \oplus V') = 0$ by Lemma 3.3, using that $p > 3$.

In the ramified case, $\pi_*$ is surjective on 2-torsion and $\pi^*$ is injective so it is even more straightforward: we have in the same way, using Riemann–Hurwitz, an $(R/2-1)$-dimensional $V$ such that $J_X[2] \oplus V \cong J_B[2] \oplus J_B[2]$ and again $n_{\text{wild}}(V) = 0$ by Lemma 3.3, using that $p > R$.

The second claim is equivalent because $n_{B,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}})$ and $n_{X,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}+\varepsilon})$ by Lemma 3.12. □

We now treat the case of cyclic covers $C_q$ for odd primes $q$, writing $\tau$ for a generator of $C_q$.

**Proposition 4.2.** *Consider a $C_q$ cover of curves $\pi : X \to B$ over a finite extension of $\mathbb{Q}_p$. Write $R_q$ for the number of ramification points. If $p > \max\{q, (R_q-2)(q-1)+1\}$, then*

$$n_{X,\text{wild}} = q \cdot n_{B,\text{wild}}.$$

*Equivalently, for $\rho$ a non-trivial irreducible representation of $C_q$, we have*

$$n_{\text{wild}}(X^{\rho}) = n_{\text{wild}}(X^{\mathbb{1}}).$$

*Proof.* By Riemann–Hurwitz we have $g_X = q \cdot g_B + (R_q - 2)(q-1)/2$.

Now, as an endomorphism on $\mathrm{Prym}(\pi)$, the map $(1-\tau)^{q-1}$ differs from $[q]$ by a unit. This can be seen because $\mathbb{Z}[\zeta_q]$ embeds into $\mathrm{End}(\mathrm{Prym}(\pi))$ by sending $\zeta_q$ to $\tau$. Therefore $\mathrm{Prym}(\pi)[1-\tau]$, the kernel of $1-\tau$ on the Prym, has $\mathbb{F}_q$-dimension $2(g_X - g_B)/(q-1) = 2g_B + R_q - 2$ and so $\mathrm{Prym}(\pi)[(1-\tau)^j]$ has dimension $j \cdot (2g_B + R_q - 2)$.

Note that, for $R_q \geq 2$, we have $\pi^* J_B[q] \leq \mathrm{Prym}(\pi)[1-\tau]$ and so

$$\mathrm{Prym}(\pi)[1-\tau] \cong V \oplus \ker((1-\tau) \circ \pi^*)[q] \cong V \oplus J_B[q]$$

for some $(R_q - 2)$-dimensional wild inertia representation $V$ by Maschke's Theorem. In this case, for each $2 \leq i \leq q-1$, we have

$$\mathrm{Prym}(\pi)[(1-\tau)^i] / \mathrm{Prym}(\pi)[(1-\tau)^{i-1}] \cong V \oplus J_B[q].$$

To see this, note that

$$\mathrm{Prym}(\pi)[(1-\tau)^i] \xrightarrow{(1-\tau)^{i-1}} \mathrm{Im}((1-\tau)^{i-1}|_{\mathrm{Prym}(\pi)}) \cap \mathrm{Prym}(\pi)[1-\tau],$$

is surjective with kernel $\mathrm{Prym}(\pi)[(1-\tau)^{i-1}]$, and so the right-hand side is simply $\mathrm{Prym}(\pi)[1-\tau]$ by counting.

We decompose $J_X[q]$ as a wild inertia representation:

$$J_X[q] \cong J_X[q] / \ker(\pi_*)[q] \oplus \bigoplus_{i=1}^{q-1} \mathrm{Prym}(\pi)[(1-\tau)^i] / \mathrm{Prym}(\pi)[(1-\tau)^{i-1}].$$

Noticing that $J_X[q] / \ker(\pi_*)[q] \cong \pi_*(J_X[q])$, we therefore have

$$J_X[q] \cong J_B[q]^{\oplus q} \oplus V^{\oplus q-1} \tag{†}$$

as wild inertia representations and reach the first conclusion by applying Lemma 3.3 to $V^{\oplus q-1}$, using that $p > \dim V^{\oplus q-1} + 1 = (R_q - 2)(q-1) + 1$.

In the case $R_q = 0$, there is an analogous identity to (†) with the 'junk' terms instead on the left-hand side. One can see this by using the facts that $\pi^* J_B[q]$ is all of $\ker(\pi_*)[q]$ and that $\pi_* : J_X[q] \to J_B[q]$ has cokernel of dimension one, then using that $p > q$.

A monodromy argument shows that we cannot have $R_q = 1$. An alternative way to see this is that, assuming $R_q = 1$, we would have $\pi^* J_B[q] \leq \mathrm{Prym}(\pi)[1-\tau]$, but the left-hand side has dimension $2g_B$ whilst the right has dimension $2g_B - 1$.

For the second part of the proposition, apply Lemma 3.12 to write

$$n_{X,\mathrm{wild}} = n_{\mathrm{wild}}(X^{\mathbb{1}}) + \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})} n_{\mathrm{wild}}(X^{\sigma(\rho)}) \text{ and } n_{B,\mathrm{wild}} = n_{\mathrm{wild}}(X^{\mathbb{1}})$$

and conclude by Lemma 3.10, which says that these conjugate pieces have the same wild conductor exponents. □

**Remark 4.3.** In the case of superelliptic curves $X : y^n = f(x)$, we have $J_X[1-\tau]$ being generated by differences of ramification points, which are easily described: they correspond to Weierstrass points $(\alpha, 0)$ with ramification index $n/\gcd(n, m_\alpha)$, where $m_\alpha$ is the multiplicity of $\alpha$ as a root of $f$. One can show that, for a cover $X \to B$ with $B : y^{n/q} = f(x)$, the wild inertia action on $V$ is given by the actions of wild inertia on the roots of the irreducible factors of $f$ whose multiplicity $d$ satisfies $\gcd(n, d) = \gcd(n/q, d)$. The corresponding conductor exponents are measured by $w_K$. This sets up a proof of Proposition 1.8 by induction: use this description of $V$ and take wild conductor exponents on both sides of (†). ♢

4.2. **General cyclic groups.** We now consider a general $C_n$-cover of curves $X \to B$ over a finite extension of $\mathbb{Q}_p$.

**Proposition 4.4.** *Consider a $C_n$-cover of curves $\pi : X \to B$. For each prime $q \mid n$, write $R_q$ for the number of points with ramification index divisible by $q$ in this cover. For $p \nmid n$, $p > \max_{q|n}\{q, (R_q - 2)(q-1) + 1\}$, we have*

$$n_{\mathrm{wild}}(X^\rho) = n_{\mathrm{wild}}(X^{\mathbb{1}})$$

*for any irreducible $C_n$-representation $\rho$.*

*Proof.* We go by induction on $n$.

Choose prime $q \mid n$ and consider $C_q \leq C_n$. Writing $\rho'$ for a non-trivial irreducible $C_q$-representation, we have

$$n_{\mathrm{wild}}(X^{\mathrm{Ind}_{C_q}^{C_n}(\rho' - \mathbb{1})}) = 0$$

by one of Propositions 4.1 or 4.2 and Lemma 3.11, the former of which apply because the maximum number of points with ramification index $q$ in the $C_q$-subcover is $R_q$.

We may decompose $\mathrm{Ind}_{C_q}^{C_n}(\rho' - \mathbb{1})$ as some degree zero $\mathbb{Z}$-linear combination of irreducibles $\rho_i$. For non-faithful $\rho_i$ we have $n_{\mathrm{wild}}(X^{\rho_i}) = n_{\mathrm{wild}}(X^{\mathbb{1}})$ by passing to the quotient on which $\rho_i$ is faithful, by the inductive hypothesis. Note that we can pass to quotients because the quotient cover will also have at most $R_q$ points with ramification index divisible by $q$.

Now, all faithful irreducibles must appear amongst the $\rho_i$ by Frobenius reciprocity and combining with the above gives $\sum_{\rho \text{ faithful}} n_{\mathrm{wild}}(X^\rho) = \phi(n) \cdot n_{\mathrm{wild}}(X^{\mathbb{1}})$, where $\phi$ is Euler's totient function and so $\phi(n)$ is the number of faithful irreducible representations. The result follows from Lemma 3.10 because all the faithful irreducibles are conjugate. □

## 5. Symmetric covers and Theorem 1.1

The aim of this section is to establish Theorem 1.1 by piecing together relations coming from cyclic subgroups of $S_n$.

**Definition 5.1.** For a field $K$ of characteristic different from $n$, let $S_n$ act on $K^n$ by permuting the standard basis vectors. The standard irreducible representation $F = F_n$ of $S_n$ is the $(n-1)$-dimensional subspace consisting of vectors whose coefficients sum to 0.

Write $\varepsilon$ for the sign representation and, as always, $\mathbb{1}$ for the trivial irreducible representation of $S_n$. We seek to prove:

**Theorem 5.2.** *Let $X \to B$ be an $S_n$-cover of curves over a finite extension of $\mathbb{Q}_p$ with $p > n$, such that $X/S_{n-1}^\circ \to B$ is simply branched, except possibly above one branch point. We have*

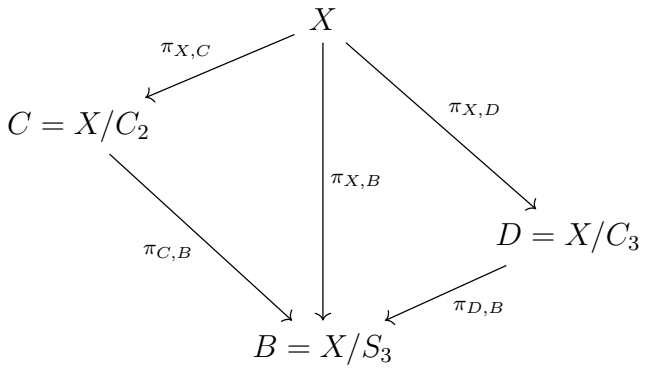
$$n_{\text{wild}}(X^F) = (n-2) \cdot n_{\text{wild}}(X^{\mathbb{1}}) + n_{\text{wild}}(X^\varepsilon).$$

Once we have proved Theorem 5.2, Theorem 1.1 will easily follow:

*Proof of Theorem 1.1.* By [2, Corollary 3.2], a simply branched cover $C \to \mathbb{P}^1$ of degree $n$ has $S_n$-Galois closure, say $X$. We take $D = X/A_n$. After using Lemma 3.12 to write $n_{C,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}+F})$ and $n_{D,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}\oplus\varepsilon})$—and noting that $n_{\text{wild}}(X^{\mathbb{1}}) = n_{\mathbb{P}^1,\text{wild}} = 0$—we have $n_{C,\text{wild}} = n_{D,\text{wild}}$ from the simply branched case of Theorem 5.2. Finally, taking another hyperelliptic curve with the same branch locus just replaces $D$ by a quadratic twist $D'$, whose Jacobian has isomorphic 2-torsion to that of $D$ and so the same wild conductor exponent. □

5.1. **The case $n = 3$.** The case of $S_3$-covers is particularly interesting for two reasons; because in some instances we can extract more information than about just the wild inertia action, and because it affords generalisation to dihedral groups.

Consider an $S_3$-cover of curves $\pi : X \to B$ over a finite extension of $\mathbb{Q}_p$, labelling the quotients as in the diagram below.




By Proposition 4.2, we have $n_{\text{wild}}(X^\rho) = n_{\text{wild}}(X^{\mathbb{1}_{C_3}})$ for $p > \max\{3, 2(R_3 - 2)\}$, where $R_3$ is the number of ramification points in the quotient cover $X \to D$. Applying Lemma 3.11, we obtain a relation

$$n_{\text{wild}}(X^{\text{Ind}_{C_3}^{S_3}(\rho - \mathbb{1}_{C_3})}) = n_{\text{wild}}(X^{F_3 - \mathbb{1} - \varepsilon}) = 0.$$

After noting that $C \to \mathbb{P}^1$ being non-simply branched above a single point corresponds to $R_3 = 2$ (e.g. by Riemann–Hurwitz), this is precisely the case $n = 3$ of Theorem 5.2. In particular, we find

$$J_C[3] \sim J_B[3] \oplus J_D[3]$$

as wild inertia representations, where $\sim$ denotes isomorphism up to trivials. In this case we can, however, go beyond a statement about wild inertia.

**Proposition 5.3.** *Let $X \to \mathbb{P}^1$ be an $S_3$-cover of curves and let $R$ be the number of points of ramification index 3 in the quotient cover $C \to \mathbb{P}^1$. For any choice of $\langle\tau\rangle \cong C_3 \leq S_3$, the $G_K$-module map*

$$(\ddagger) \qquad (1-\tau)\circ\pi_{X,C}^* : J_C[3] \to J_X[3]$$

*has image landing in $\pi_{X,D}^* J_D[3]$, into/onto which it is*

*(1) an injection if $R = 0$ (equivalently, if $g_C = g_D - 1$);*
*(2) an isomorphism if $R = 1$ (equivalently, if $g_C = g_D$).*

*Proof.* Firstly we show that the image lands in $\pi_{X,D}^* J_D[3]$: to see this, first note that a point $P$ in the image satisfies $(1-\tau)(P) = 0$ (because $(1-\tau)^2 \equiv 1 + \tau + \tau^2 - 3\tau \pmod 3$), i.e. the image lies in $\ker(1-\tau)|_{\ker(\pi_{X,D,*})[3]}$, which contains $\pi_{X,D}^* J_D[3]$.

In the $R = 1$ case, a Riemann–Hurwitz calculation shows that $g_C = g_D$ and that $\pi_{X,D}$ is branched over exactly two points. As in the proof of Proposition 4.2, we have $\ker(1-\tau)|_{\ker(\pi_{X,D,*})[3]} = \mathrm{Prym}(\pi_{X,D})[1-\tau]$ having dimension $2g_D$ and so this space is $\pi_{X,D}^* J_D[3]$.

In the $R = 0$ case, we have $g_C = g_D - 1$ and $\pi_{X,D}$ being unramified. Here we have $\ker(1-\tau)|_{\ker(\pi_{X,D,*})[3]}$ of dimension at most one more than $\mathrm{Prym}(\pi_{X,D})[1-\tau]$ by Proposition 3.7, which has dimension $2g_D - 2$ as in the proof of Proposition 4.2. Moreover, the former contains $\pi_{X,D}^* J_D[3]$ of dimension $2g_D - 1$, so we must again have $\ker(1-\tau)|_{\ker(\pi_{X,D,*})[3]} = \pi_{X,D}^* J_D[3]$.

We now think of the codomain of $(\ddagger)$ as being $\pi_{X,D}^* J_D[3]$: in the $R = 1$ case, the space of points $P \in J_C[3]$ such that $\pi_{X,C}^* P$ is fixed by $\tau$ is trivial because $\pi_{X,D}^* J_D[3]$ intersects trivially with $\pi_{X,C}^* J_C[3]$. To see this, note that $\pi_{X,C}^* P = \pi_{X,D}^* Q$ implies $2P = 0$ by applying $\pi_{X,C,*}$ to both sides. It immediately follows that the map must be an isomorphism.

The claim in the unramified case follows from the same observation, which also shows that no points in $\pi_{X,C}^* J_C[3]$ can be fixed by $\tau$. □

**Remark 5.4.** One could also state a version of Proposition 5.3 for $R \geq 2$, in which case $(\ddagger)$ would have image $\pi_{X,D}^* J_D[3]$, but the details of such a proof grow increasingly cumbersome. ♢

**Remark 5.5.** In the case of an elliptic curve $C : y^2 = x^3 + ax + b$, $a \neq 0$, equipped with the cover $x : C \to \mathbb{P}^1$, we recover the known isomorphism of Galois modules between $C[3]$ and $J_D[3]$. To the best of the author's knowledge, this observation first appeared in the literature as [8, Lemma 6.9 + Remark 6.10], where they study the kernel of an isogeny $J_C^2 \times J_D \to J_X$. ♢

**Remark 5.6.** For an odd prime $q$ and a $D_{2q}$-cover $X \to B$, where $D_{2q}$ is the dihedral group of order $2q$, with quotients labelled analogously to the above, one can similarly show

$$J_C[q] \sim J_B[q] \oplus J_D[q]^{\oplus(q-1)/2}$$

using the techniques of Proposition 4.2. Moreover, when $R_q = 1$, we have equality on wild conductor exponents between $J_C$ and $J_B \times J_D^{(q-1)/2}$ for all primes different from $q$. This is an alternative generalisation of the case $n = 3$ of Theorem 5.2. ♢

5.2. **The general case.** We prove Theorem 5.2 in the general case by inducing relations from cyclic subgroups. First we prove some required Galois and representation-theoretic lemmata.

**Lemma 5.7.** *Let $X \to B$ be an $S_n$-cover such that $\pi : X/S_{n-1}^\circ \to B$ is simply branched, except possibly above one branch point. If $C_m \leq S_n$ contains*

*no transposition, then for any $q \mid m$, the cover $X \to X/C_m$ has at most $\lfloor n/q \rfloor$ points with ramification index divisible by $q$. Moreover, when $\pi$ is simply branched, this cover is unramified.*

*Proof.* Fix a point $P \in B$, and choose a point $\mathfrak{P}$ on $X$ lying above $P$. The points above $P$ on $X/S^\circ_{n-1}$ correspond to the orbits of $\{1, \dots, n\}$ under the action of the decomposition group at $\mathfrak{P}$. The assumption that $X/S^\circ_{n-1} \to B$ is simply branched away from a particular branch point thereby implies that, as we vary over $P$, each decomposition group is either trivial or generated by a transposition, except for those above this branch point.

The result follows because all decomposition groups of $X \to X/C_m$ are trivial, except possibly those of the points above this branch point. □

The following is essentially a version of Artin's Induction Theorem (cf. [17, §9.2]).

**Lemma 5.8.** *Given a virtual character $\chi$ of $S_n$ with degree 0, there exists non-zero integers $a_i$, not-necessarily-distinct cyclic subgroups $H_i$ and virtual characters $\Theta_i$ of the form*

$$\Theta_i = \rho - \mathbb{1}_{H_i},$$

*where $\rho$ is an irreducible $H_i$-representation, such that*

$$a_0 \cdot \chi = \sum_i a_i \cdot \mathrm{Ind}_{H_i}^{S_n} \Theta_i.$$

*Proof.* Suppose $\langle \chi, \mathrm{Ind}_H^{S_n} \Theta \rangle = 0$ for all cyclic subgroups $H$ and possible characters $\Theta$ of this form. It suffices to show that $\chi = 0$.

Given a cycle type, choose a permutation of this type and let $H$ be the subgroup generated by this permutation. We have $\langle \mathrm{Res}_H \chi, \Theta \rangle = 0$ for all characters $\Theta$ of $H$ of the above form, by assumption. Therefore $\mathrm{Res}_H \chi = 0$ because these $\Theta$ obviously generate the set of characters of $H$ with degree 0. Thus $\chi$ vanishes on every conjugacy class. □

Before proving Theorem 5.2, we single out the special case of $C_2 \leq S_n$ generated by a transposition.

**Lemma 5.9.** *Let $C_2 \leq S_n$ be generated by a transposition. We have*

$$\mathrm{Res}_{C_2}(F_n - \varepsilon - (n-2) \cdot \mathbb{1}) = 0.$$

*Proof.* First note that, when $n = 3$, we have $\mathrm{Res}_{C_2}(F_3) = \mathbb{1}_{C_2} \oplus \varepsilon_{C_2}$, where $\varepsilon_{C_2}$ is the non-trivial irreducible of $C_2$.

For general $n$, restricting to $S^\circ_{n-1}$ gives $\mathrm{Res}_{S^\circ_{n-1}} F_n = F_{n-1} + \mathbb{1}_{S^\circ_{n-1}}$ by Frobenius reciprocity, and the result follows by induction. □

We are now ready to prove Theorem 5.2.

*Proof of Theorem 5.2.* We treat the simply branched case:

Note that $F - \varepsilon - (n-2) \cdot \mathbb{1}$ has degree 0, so we may find $a_i$, $H_i$ and $\Theta_i$ as in Lemma 5.8 such that

$$(*) \qquad a_0 \cdot (F - \varepsilon - (n-2) \cdot \mathbb{1}) = \sum_i a_i \cdot \mathrm{Ind}_{H_i}^{S_n} \Theta_i.$$

If $H_i$ contains no transpositions, then $n_{\mathrm{wild}}(X^{\mathrm{Ind}_{H_i}^{S_n} \Theta_i}) = 0$ by Lemma 3.11 and Proposition 4.4, which applies by Lemma 5.7. The cycle types which generate subgroups containing transpositions are transpositions themselves along with the product of cycles of odd lengths with a transposition. By Frobenius reciprocity and the same reasoning as above, if we show that $\mathrm{Res}_H(F - \varepsilon - (n-2) \cdot \mathbb{1})$

is the lift of a representation from a subgroup containing no transposition for each $H$ generated by a cycle of such a type, then we will have $n_{\text{wild}}(RHS) = 0$, where $RHS$ is the right-hand side of $(*)$, and may conclude.

By Lemma 5.9 and Frobenius reciprocity, we may assume that none of the $H_i$ appearing in $(*)$ are generated by a single transposition. For the case of the product of a transposition with cycles of odd length, write $2m$ for the order of such a permutation and $C_{2m} = C_2 \times C_m$ for the corresponding subgroup. Now, Lemma 5.9 applied to $C_2 \leq C_2 \times C_m$ gives $\text{Res}_{C_2} F = (n-2) \cdot \mathbb{1}_{C_2} + \varepsilon_{C_2}$, so $\text{Res}_{C_2 \times C_m} F$ is a sum of $(n-2)$ irreducibles lifted from $C_m$ and one irreducible representation which restricts to $\varepsilon_{C_2}$ on $C_2$, which must be $\text{Res}_{C_2 \times C_m} \varepsilon$ because $F$ is rational. Therefore, $\text{Res}_{C_{2m}}(F - \varepsilon - (n-2) \cdot \mathbb{1})$ is in the space generated by characters lifted from the subgroup $C_m$ containing no transpositions.

The other case is almost identical, but $C_m \leq S_n$ may have up to $\lfloor n/q \rfloor$ ramification points with ramification index divisible by $q$ by Lemma 5.7. Plugging this into the bounds from Proposition 4.4 shows that we may use the proposition in the same way as in the unramified case because we are assuming $p > n$. □

**Remark 5.10.** In the case $n = 3$, we saw that we have a $G_K$-module isomorphism (‡) when $B = \mathbb{P}^1$ and there is precisely one point with ramification index 3. In this case we also have equality, for example, between the wild conductor exponents at 2.

In this sense Theorem 5.2 is the best one could hope for when $n > 3$ because we must use relations on $q$-torsion for all $q < n$ prime, but this process obscures the conductor exponent at each such $q$. ♢

**Remark 5.11.** It is a result credited by Fulton to Severi ([9, Proposition 8.1]) that a curve $C$ over an algebraically closed field admits a simply branched degree $g_C + 1$ cover of $\mathbb{P}^1$. In the case of curves over finite extensions of $\mathbb{Q}_p$, we can ensure that such covers are defined over finite tame extensions. Thereby one could use Theorem 5.2 and Lemma 3.4 to compute wild conductor exponents for $p > g_C + 1$. In practice, given a particular curve, a perturbation argument similar to that in the sequel would likely work for smaller $p$. ♢

## 6. Perturbations and Theorem 1.4

In this section we institute a change of perspective: instead of considering a Galois cover $X \to B$, we consider a non-Galois cover of degree $n$ from $C \to B$ and its Galois-closure $X$. Further, we restrict to the case that $B = \mathbb{P}^1$. Note that (at least generically) $C$ plays the role of $X/S_{n-1}^{\circ}$ as in the preceding sections.

Recall the following piece of notation.

**Notation.** For $K$ a finite extension of $\mathbb{Q}_p$ and a polynomial $g \in K[t]$ write

$$w_K(g) = \sum_{r \in R/G_K} m(r) \cdot (v_K(\Delta_{K(r)/K}) - [K(r) : K] + f_{K(r)/K}),$$

where $R$ is the set of roots of $g$ over $\overline{K}$ and $m(r)$ is the multiplicity of $r$.

This quantity will arise because of its connection to wild conductor exponents of hyperelliptic curves.

**Theorem 6.1** (=[6, Theorem 11.3])**.** *Let $C/K : y^2 = f(x)$, for square-free $f$, be a hyperelliptic curve over a finite extension of $\mathbb{Q}_p$ with $p$ odd.*

$$n_{C,\text{wild}} = w_K(f).$$

**Remark 6.2.** Note that $w_K(f) = w_K(\mathrm{disc}_y(y^2 - f(x)))$ because these polynomials differ by multiplication by a constant, so Theorem 6.5 is a direct generalisation of Theorem 6.1.

Theorem 6.1 is proved by observing that the wild inertia action on 2-torsion of a hyperelliptic curve $y^2 = f(x)$ is isomorphic to the wild inertia action on the roots of $f$. This relies on the explicit description of the 2-torsion of such a curve, whilst Theorem 6.5 does not rely on any explicit knowledge of torsion; we reduce to the explicit description of 2-torsion on some auxiliary hyperelliptic discriminant curve after perturbation. ♢

Fixing some finite extension $K$ of $\mathbb{Q}_p$, we first prove an important local constancy property of the quantity $w_K$.

**Lemma 6.3.** *Let $g \in K[t]$ be $p^{th}$-power-free and suppose square-free $h \in K[t]$ is sufficiently close to $g$, in the sense that all of their coefficients are $p$-adically close. We have $w_K(h) = w_K(g)$.*

*Proof.* From the proof of [6, Theorem 11.3], when $g$ is square-free $w_K(g)$ is determined by the action of the wild inertia group $W_K$ on $\mathbb{Q}_2[R]$, where $R$ is the set of roots of $g$ over $\overline{K}$.

Suppose $g = \prod_i g_i^{e_i}$ for distinct irreducible $g_i$ and $e_i \leq p-1$. Write $R_i$ for the roots of $g_i$ over $\overline{K}$ and $R_h$ for those of $h$. We claim that $\mathbb{Q}_2[R_h] \cong \bigoplus_i \mathbb{Q}_2[R_i]^{\oplus e_i}$ as $W_K$-representations, so $w_K(h) = w_K(g)$:

Firstly recall that $W_K$ acts via a finite $p$-group, and so each orbit under the action of $W_K$ has size a power of $p$.

Choose $r \in R_h$ and note that $r$ is close to a point in $r_0 \in R_i$ for some $i$. In fact, there is a small neighbourhood of $r_0$ containing $e_i$ points. By continuity of the $W_K$-action, given such a neighbourhood of each $r_0 \in R_i$, there is an orbit of these neighbourhoods mirroring the orbit of $r_0$. Supposing that the orbit of $r$ contains more than one point in any of these neighbourhoods leads to a contradiction: we would have

$$|W_K \cdot r_0| < |W_K \cdot r| \leq |W_K \cdot r_0| \cdot e_i \leq |W_K \cdot r_0| \cdot (p-1),$$

but this shows that $|W_K \cdot r_0|$ and $|W_K \cdot r|$ cannot both be powers of $p$.

To conclude, we have shown that for each $W_K$-orbit of roots of $g_i$ we obtain $e_i$ distinct orbits of points in $R_h$, each defining a representation isomorphic to that of the original orbit. □

To prove our main theorem, we will need to distinguish between an affine curve $\mathcal{C}/K : f(x,y) = 0$ and its smooth projective normalisation $C$. The following lemma will help us reduce to the case of Theorem 5.2.

**Lemma 6.4.** *Suppose $\mathcal{C}/K : f(x,y) = 0$ is smooth away from infinity and is such that $g_C > 0$. We can choose $\widetilde{f}(x,y)$ with coefficients arbitrarily close to those of $f$ such that $\widetilde{\mathcal{C}}/K : \widetilde{f}(x,y) = 0$ with normalisation $\widetilde{C}$ satisfies $g_C = g_{\widetilde{C}}$, and $y : \widetilde{\mathcal{C}} \to \mathbb{A}^1$ is simply branched.*

*Proof.* Write $n = \deg_x f$ and define $f_{\boldsymbol{\varepsilon}}(x,y) = f(x,y) + \sum_{i=0}^{n-1} \varepsilon_i x^i$, where $\boldsymbol{\varepsilon} = (\varepsilon_0, \ldots, \varepsilon_{n-1})$ takes values in $\overline{K}^n$, noting that perturbing in this way will not affect the behaviour at infinity.

It suffices to show that $\mathrm{disc}_y \mathrm{disc}_x f_{\boldsymbol{\varepsilon}}(x,y) \neq 0$ as a polynomial in the $\varepsilon_i$. Indeed, in that case we can choose $\boldsymbol{\varepsilon} \in K^n$ small such that this polynomial does not vanish, which precisely means that $\mathrm{disc}_x f_{\boldsymbol{\varepsilon}}$ has no repeated root, so projection onto $y$ from the affine curve $f_{\boldsymbol{\varepsilon}}(x,y) = 0$ is a simply branched cover of $\mathbb{A}^1$. To do this, we show that such an affine curve can be explicitly constructed with $\boldsymbol{\varepsilon} \in \overline{K}^n$.

Write $B$ for the set of branch points and $B' \subseteq B$ for the set of non-simple finite branch points of $C \to \mathbb{P}^1$:

Choose a non-simple branch point $b \in B'$ and $\alpha$ a double root of $f(x,b)$. Take $f_{\boldsymbol{\varepsilon}}(x,y) = f(x,y)+\delta(x-\alpha)^2$. For $\delta$ sufficiently small, $f_{\boldsymbol{\varepsilon}}(x,y) = 0$ defines a curve of the same genus for which projection onto $y$ is simply branched at $b$. This is because $f(x,b) + \delta(x-\alpha)^2 = (x-\alpha)^2(g(x)+\delta)$ for some polynomial $g$, and now $g(x)+\delta$ is square-free so long as $\delta \neq -g(\beta)$ for $\beta$ any root of $g'$.

Note that $\operatorname{disc}_x f_{\boldsymbol{\varepsilon}}(x,y)$ varies continuously with $\boldsymbol{\varepsilon}$ and hence so do the roots, which are the branch points counted with multiplicity $\sum_{P\in y^{-1}(b)}(e_P-1)$. For small enough $\delta$, then, there is a single simple branch point of $f_{\boldsymbol{\varepsilon}}(x,y) = 0$ in a small neighbourhood of each finite simple branch point of $C$.

Because the genera are the same by the degree-genus formula, the sum $\sum_{b\in B\setminus B'}\sum_{P\in y^{-1}(b)}(e_P-1)+\sum_{b\in B'}\sum_{P\in y^{-1}(b)}(e_P-1)$ is constant by Riemann–Hurwitz. The number of simple branch points has increased, so the quantity $\sum_{b\in B'}\sum_{P\in y^{-1}(b)}(e_P-1)$ has decreased, and iterating this process eventually gives the desired affine curve $f_{\boldsymbol{\varepsilon}}(x,y) = 0$ defined over $\overline{K}$. □

Finally, we are able to show Theorem 1.4.

**Theorem 6.5.** *Let $\mathcal{C} : f(x,y) = 0$ be a smooth affine curve over a finite extension $K$ of $\mathbb{Q}_p$ with normalisation $C$. If $p > \deg_x f = n$, then*

$$n_{C,\text{wild}} = w_K(\operatorname{disc}_x f).$$

*Proof.* Consider the map $\pi : C \to \mathbb{P}^1$ corresponding to $y : \mathcal{C} \to \mathbb{A}^1$. When this has $S_n$-Galois closure $X$, the curve $D = X/A_n$ is the hyperelliptic curve given by $D : \Delta^2 = \operatorname{disc}_x f$. The smoothness of $\mathcal{C}$ guarantees that

$$(**) \qquad \operatorname{disc}_x f = u \cdot \prod_{t\in\mathbb{P}^1}\prod_{P\in\pi^{-1}(t)}(y-t)^{e_P-1}$$

for some $u \in K^\times$, where $e_P$ is the ramification index at $P$ and '$y-\infty$' is taken to be 1. Note that without the assumption on smoothness, the right-hand side of $(**)$ need only divide the left. As in the proof of Theorem 1.1, Lemma 3.12 gives $n_{C,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}+F})$ and $n_{D,\text{wild}} = n_{\text{wild}}(X^{\mathbb{1}+\varepsilon})$. We have $n_{\text{wild}}(X^{\mathbb{1}}) = 0$ and so, when $y : \mathcal{C} \to \mathbb{A}^1$ is simply branched, Theorem 5.2 ensures that $n_{C,\text{wild}} = n_{D,\text{wild}}$. The conclusion follows from Theorem 6.1, using that $\operatorname{disc}_x f$ is square-free.

To reduce to this case, we first perturb the equation $f(x,y) = 0$ as in Lemma 6.4 to obtain $\widetilde{C} : \widetilde{f}(x,y) = 0$ with corresponding cover $y : \widetilde{\mathcal{C}} \to \mathbb{A}^1$ simply branched. If $\operatorname{Gal}(\widetilde{f}) \cong S_n$ as a polynomial over $\overline{K}(y)$, then we are done. We can ensure this is the case using the same perturbations as in Lemma 6.4: if $\operatorname{Gal}(\widetilde{f}) \ncong S_n$, then $\operatorname{Gal}(\widetilde{f}_{\boldsymbol{\varepsilon}}(x,y_0)) \lneq S_n$ for any choice of $y_0$, but now fix $y_0$ and choose $\boldsymbol{\varepsilon}'$ small with respect to $v_K$ such that $\operatorname{Gal}(\widetilde{f}_{\boldsymbol{\varepsilon}'}(x,y_0)) \cong S_n$, which is easily done. Because the roots of $\operatorname{disc}_x f_{\boldsymbol{\varepsilon}}$ vary continuously with $\boldsymbol{\varepsilon}$, this sufficiently small perturbation will not introduce any non-simple branching.

We conclude by Lemma 6.3 and the local constancy of wild conductor exponents [10, Theorem 5.1(1)]. The former applies because $\operatorname{disc}_x f$ is $n^{\text{th}}$-power-free by $(**)$ and $p > n$. The latter applies because perturbing in the described way yields an $\ell$-adic family of curves of generic genus $g_C$. □

**Corollary 6.6.** *Consider a superelliptic curve $C/K : y^n = f(x)$, $f$ square-free, over a finite extension $K$ of $\mathbb{Q}_p$. If $p > n$, then*

$$n_{C,\text{wild}} = (n-1)\cdot w_K(f).$$

*Proof.* Note that $\mathrm{disc}_y(y^n - f(x))$ is a constant multiple of $f^{n-1}$. After relabelling $x$ and $y$, we are in the case described in Theorem 6.5. □

## Appendix A. 3-torsion of genus 2 curves

The following is [7, Proposition 4.1], which is used in *loc. cit.* to compute wild conductor exponents at $p = 2$ of genus 2 curves.

> *Let $C/k$ be a genus 2 curve over a field of characteristic different from 2 and 3 with model $y^2 = F(x)$. There is a one-to-one correspondence between the non-zero 3-torsion points of the Jacobian variety $J_C$ and tuples $(u_1, \dots, u_7) \in \overline{k}^7$ such that*
>
> $$F(x) = (u_4x^3 + u_3x^2 + u_2x + u_1)^2 - u_7(x^2 + u_6x + u_5)^3.$$
>
> *Moreover, this correspondence preserves the action of the absolute Galois group $G_k$.*

It turns out that this sometimes fails to pick up all 3-torsion points.

**Example A.1.** Consider the curve with LMFDB [12] label 1744.a.1744.1 which has model

$$C/\mathbb{Q}: \quad y^2 = F(x) = (x^3 + x)(x^3 + x + 4),$$

so $J_C(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$. According to the above, we should expect two rational solutions to the system of equations described, but a check using Magma proves that there are none. Indeed, there are only 78 solutions to this system of equations over $\overline{\mathbb{Q}}$. ♢

A corrected version is as follows.

**Proposition A.2.** *Let $C/k$ be a genus 2 curve over a field of characteristic different from 2 and 3 with model $y^2 = F(x)$. There is a one-to-one correspondence between the non-zero 3-torsion points of $J_C$ and the union of the sets:*

*(1) Tuples $(u_1, u_2, u_3, u_4, u_5, u_6, u_7) \in \overline{k}^7$ such that*
$$F(x) = (u_4x^3 + u_3x^2 + u_2x + u_1)^2 - u_7(x^2 + u_6x + u_5)^3;$$

*(2) Tuples $(v_1, v_2, v_3, v_4, v_5, v_6) \in \overline{k}^6$ such that*
$$F(x) = (v_4x^3 + v_3x^2 + v_2x + v_1)^2 - v_6(x + v_5)^3;$$

*(3) Tuples $(w_1, w_2, w_3, w_4, w_5) \in \overline{k}^5$ such that*
$$F(x) = (w_4x^3 + w_3x^2 + w_2x + w_1)^2 - w_5.$$

*Moreover, this correspondence preserves the action of $G_k$.*

*Proof.* Suppose $\mathcal{D}$ is a divisor on $C$ such that $3\mathcal{D}$ is principal. Explicitly,

$$\mathcal{D} = (P_1) + (P_2) - (\infty_1) - (\infty_2), \qquad P_i = (X_i, Y_i) \text{ or } P_i \in \{\infty_{1,2}\}$$

for some points $P_i$ on $C$ and where $\infty_{1,2}$ are the not-necessarily-distinct points at infinity. There exists some rational function $g$ with $\mathrm{div}(g) = 3D$. Then $g$ is in the Riemann–Roch space $L(3(\infty_1) + 3(\infty_2)) = \langle 1, x, x^2, x^3, y\rangle$. It is easy to see that the coefficient of $y$ must be non-zero and so

$$g = y + a_3x^3 + a_2x^2 + a_1x + a_0$$

after a suitable re-scaling.

Taking norms from $k(C)$ to $k(x)$ yields a function $(a_3x^3+a_2x^2+a_1x+a_0)^2-F(x)$ on $\mathbb{P}^1$, for some $a_i$, with divisor $3(X_1)+3(X_2)-6(\infty)$ a cube. Provided $C$ does not admit a degree 3 map to $\mathbb{P}^1$, we have, for some $b_j$,

$$(a_3x^3+a_2x^2+a_1x+a_0)^2-F(x)=b_2(x^2+b_1x+b_0)^3.$$

We needed this assumption to avoid the case that $P_i=\infty_j$ for some $i,j$. In this case we have, without loss of generality,

$$\mathcal{D}=(P_1)-(\infty_1), \qquad \operatorname{div}(g)=3(P_1)-3(\infty_1)$$

and $g:C\to\mathbb{P}^1$ is a degree 3 map.

Now the norm map yields a function as above which is still a cube, but now has divisor $3(X_1)-3(\infty)$. Hence we conclude that

$$(a_3x^3+a_2x^2+a_1x+a_0)^2-F(x)=b_1(x+b_0)^3,$$

for some $b_j$, unless $P_1=\infty_2$. In this final case the norm map yields a constant function and so we conclude that

$$(a_3x^3+a_2x^2+a_1x+a_0)^2-F(x)=b,$$

for some $b$. □

Note that the original result is correct if one starts with $\deg F$ being odd, with such a model existing whenever $C$ has a rational point. The troublesome cases for which it may fail are those curves admitting degree 3 covers $\pi:C\to\mathbb{P}^1$ with associated 'discriminant curve' of genus at most 1. By this we refer (up to quadratic twist) to the curve

$$D:\ \ y^2=\prod_{t\in\mathbb{P}^1}\prod_{P\in\pi^{-1}(t)}(x-t)^{e_P-1},$$

as in $(**)$ from the proof of Theorem 6.5. Examples of curves $C$ admitting such covers are mentioned in [4, Example 2]. That these are the troublesome cases can be seen from the following lemma.

**Lemma A.3.** *Let $C/k$ be a genus 2 curve. There is a divisor $\mathcal{D}$ on $C$ of the form*

$$\mathcal{D}=(P)-(Q)$$

*corresponding to a non-zero element of $J_C[3]$ if and only if $C$ admits a degree 3 cover of $\mathbb{P}^1$ which is non-simply branched above at least two points, or equivalently such that the corresponding discriminant curve $D$ has genus strictly less than 2.*

*Proof.* For the 'if' direction, suppose that we are given $\pi:C\to\mathbb{P}^1$ of degree 3 such that the corresponding discriminant curve $D$ has genus less than 2. Writing $R_2$ for the number of simple branch points and $R_3$ for the number of non-simple branch points of $\pi$, we have $8=R_2+2R_3$ and $g_D=-1+R_2/2$ by Riemann–Hurwitz. This implies that $\pi$ is non-simply branched above at least two points, say $t_1$ and $t_2$. After a translation sending $t_1$ to 0 and $t_2$ to $\infty$, the divisor $\mathcal{D}=\operatorname{div}(\pi)/3$ of the claimed form lies in $J_C[3]$.

For the 'only if' direction, suppose $\mathcal{D}=(P)-(Q)$ is in $J_C[3]$. Then there exists $\pi:C\to\mathbb{P}^1$ with $\operatorname{div}(\pi)=3(P)-3(Q)$. This says that $\pi$ has degree 3 and is non-simply branched above 0 and above $\infty$.

The equivalence of the branching condition and the condition on the genus of $D$ follows from a Riemann–Hurwitz calculation. □

## References


[1] Daniele Agostini. On the Prym map for cyclic covers of genus two curves. *Journal of Pure and Applied Algebra*, 224:106384, 04 2020.

[2] Indranil Biswas, Manish Kumar, and A. J. Parameswaran. Genuinely ramified maps and monodromy. *Journal of Algebra*, 644, 2024.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma Algebra System I: The User Language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[4] Nils Bruin, E. Victor Flynn, and Damiano Testa. Descent via (3,3)-isogeny on Jacobians of genus 2 curves. *Acta Arithmetica*, 165, 2014.

[5] Brian Conrad and William A. Stein. Component Groups of Purely Toric Quotients. *Mathematical Research Letters*, 8(6):745–766, 2001.

[6] Tim Dokchitser, Vladimir Dokchitser, Celine Maistret, and Adam Morgan. Arithmetic of hyperelliptic curves over local fields. *Mathematische Annalen*, 385:1213–1322, 2022.

[7] Tim Dokchitser and Christopher Doris. 3-torsion and conductor of genus 2 curves. *Mathematics of Computation*, 88, 2017.

[8] Vladimir Dokchitser, Holly Green, Alexandros Konstantinou, and Adam Morgan. Parity of ranks of Jacobians of curves. *Proceedings of the London Mathematical Society*, 131, 2025.

[9] William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Annals of Mathematics*, 90(3):542–575, 1969.

[10] Mark Kisin. Local constancy in $p$-adic families of Galois representations. *Mathematische Zeitschrift*, 230:569–593, 1999.

[11] Roman Kohls. *Conductors of superelliptic curves*. PhD thesis, Universität Ulm, 2019.

[12] The LMFDB Collaboration. The $L$-functions and modular forms database. `https://www.lmfdb.org`.

[13] Elvira Lupoian. Two-torsion subgroups of some modular Jacobians. *International Journal of Number Theory*, 20(10):2543–2573, 2024.

[14] Elvira Lupoian. Three-torsion subgroups and wild conductors of genus 3 hyperelliptic curves. *Journal of Number Theory*, 278:267–284, 2026.

[15] Elvira Lupoian and James Rawson. Three-torsion subgroups and wild conductor exponents of plane quartics. *Research in Number Theory*, 11, 2025.

[16] Michael Rosen. The norm map on Jacobians. *Proceedings of the American Mathematical Society*, 87(1):19–22, 1983.

[17] Jean-Pierre Serre. *Linear representations of finite groups*. Springer-Verlag, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[18] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88(3):492–517, 1968.

[19] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer–Verlag, 1994.

[20] Douglas Ulmer. Conductors of $\ell$-adic representations. In *Proceedings of the American Mathematical Society*, volume 144, 2016.



University College, London, WC1H 0AY, UK
*Email address*: `harry.spencer.22@ucl.ac.uk`