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

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 π is a uniformiser, and n_C is the *conductor exponent*. In turn, n_C is defined to be

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

where the *tame conductor exponent*, $n_{C,\mathrm{tame}}$, 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 ℓ-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 [17, Chapter 4]. For hyperelliptic curves the problem is solved for $p \neq 2$ by means of an explicit formula in [4, Theorem 11.3]. In [12] the problem is solved for $p \neq 2$ for curves of genus at most 5. In [5, §4], by providing an algorithm for the explicit computation of 3-torsion (cf. §A), the problem is solved for genus 2 curves, and in [11, §3] the problem is solved for hyperelliptic genus 3 curves analogously. The problem is solved for plane quartics with a rational point in [13, Theorem 2]. A formula is given in [9, 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 (=Theorem 5.2)**.** *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 $p > n$. The hyperelliptic curve D defined by the ramification locuss satisfies*

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

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 5.9. ♢

In fact, we prove a stronger result 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 $(n-1)\cdot n_{B,\mathrm{wild}}$, allowing a slightly weaker restriction on ramification.

By appealing to [4, 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 analagous formula for some plane curves. In fact, [4, 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 is the set of roots 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 [2]. ♢

Theorem 1.4 (=Theorem 6.5)**.** *Let $C : f(x, y) = 0$ be a model which is smooth away from infinity for a curve over a finite extension K of $\mathbb{Q}_p$. If $p > \deg_x f$, then*

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

Remark 1.5. To prove Theorem 6.5 we need a stronger version of Theorem 1.1 which allows one branch point above which our cover 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. [1, Corollary 3.2]), and usually so do curves satisfying this less strict criterion. ♢

Remark 1.6. Given a curve embedded smoothly in $\mathbb{P}^n$ equipped with a cover of $\mathbb{P}^1$, one could obtain a similar result using a polynomial defined by the ramification locus instead of the discriminant in Theorem 1.4, provided that one can perturb the defining equations to obtain a simply branched cover. ♢

For example, Theorem 1.4 gives a simple formula for the wild conductor exponent of superelliptic curves of exponent n for $p > n$. See [9, Theorem 4.1.4] for a more general, but more opaque, formula for conductor exponents of superelliptic curves.

Corollary 1.7 (=Corollary 6.7)**.** *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*

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

We can also apply Theorem 1.4 in 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 1.8. Consider the curve $C/\mathbb{Q}_7 : f(x,y) = 7x^3y^4 + x + y^5 + 7 = 0$ of genus 6. We compute that

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

As a sanity check, one can also compute

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

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

We use the framework of *motivic pieces of curves* set out in [6, §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 ρ, define

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

Proposition 1.9 (=Proposition 4.3)**.** *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 $p > \max_{q|n}\{q, (R_q-1)(q-1)+1\}$, for any irreducible representation ρ of C_n we have*

$$\sum_{\rho' \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})\cdot\rho} n_{\mathrm{wild}}(X^{\rho' - \mathbb{1}}) = 0.$$

In §5, using an Artin-like induction lemma, we piece together these relations, establishing Theorem 1.1. Theorem 1.4 will follow from Theorem 1.1 by combining the following local constancy result with the local constancy of wild conductor exponents (e.g. [8, Theorem 5.1(1)]).

Lemma 1.10 (=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 [5, 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 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 also thank Alexandros Konstantinou for his additional guidance and many fruitful discussions. I thank Elvira Lupoian for helpful comments on a draft, James Rawson for helpful correspondence regarding Remark 5.9, and Tim Dokchitser for helpful correspondence regarding Appendix A.

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
$T_\ell A$, $V_\ell A$	ℓ-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}	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 χ of $H \leq G$ to G
$\mathrm{Res}_H \chi$	Restriction of a character χ of G to $H \leq G$

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. [18, pages 3–4])**.** The *wild conductor exponent* of V is

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

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

In particular, $n_{\mathrm{wild}}(V)$ 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 ℓ-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 $n_{\mathrm{wild}}(V_\ell A) = 0$ for all $\ell \neq p$.*

Proof. See the proof of [16, 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 $A_1, \ldots, A_n$ and $B_1, \ldots, B_m$ 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 $n_{\mathrm{wild}}(W) = 0$.

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

Therefore each primitive root of unity appears as an eigenvalue of σ 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 σ 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 ℓ-adic representation over a finite extension K of $\mathbb{Q}_p$. Suppose K'/K is a tamely ramified extension. We have*

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

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 $\pi : X \to Y$ of curves over a field K. Functorially, we obtain an embedding of function fields $K(Y) \hookrightarrow K(X)$.

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

Given a non-Galois cover $\pi : X \to Y$, we say the *Galois closure* is the curve whose function field is the Galois closure of the extension $K(X)/K(Y)$. 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 π 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.** Mumford states the following results for C_2-covers (see [14, §3 Corollary 1, §2 (i)–(viii)]), but they easily generalise to other cyclic covers.

Proposition 3.7. *Let p be a prime and $\pi : X \to Y$ a C_p-cover of curves over a field K of characteristic 0 (or different from p). Either*

(1) π is ramified and the pull-back $\pi^* : J_Y \to J_X$ is injective, or
(2) π is unramified and $\ker \pi^* = \langle P \rangle$ for some $P \in J_Y[p]$.

We will also need the following lemma on push-forwards, after recalling the definition of *Prym varieties*. Given a cover of curves $\pi : X \to Y$, we define the Prym variety associated to π to be the connected component of $\ker(\pi_* : J_X \to J_Y)$ containing the identity, denoted $\mathrm{Prym}(\pi)$.

Lemma 3.8. *Let p be a prime and $\pi : X \to Y$ a C_p-cover of curves over a field K of characteristic 0 (or different from p). Either*

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

3.4. **Motivic pieces of curves.** We summarise the key definition and some basic properties from [6, §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 3.9 (=[6, Definition 2.3])**.** For a G-representation ρ, define

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

on which G_K acts by postcomposition. Implicitly this requires a choice of ℓ, but the usual independence properties hold (cf. [6, Corollary 2.14]).

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

Definition 3.10. For a virtual character $\chi = \sum_i r_i \rho_i$ of G, we define

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

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 ρ_1 and ρ_2 two representations of G, and τ 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 [6, 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}° 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 ε 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 Lemma 3.8. We can apply Maschke's theorem (e.g. [15, 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 $J_X[2] \oplus V \cong J_B[2] \oplus \ker \pi_*[2]$.

Now $\pi^* J_B[2] \leq \ker \pi_*[2]$, so we have some two-dimensional V' such that $J_X[2] \oplus V' \cong J_B[2] \oplus J_B[2]$. We have $n_{\mathrm{wild}}(V') = 0$ by Lemma 3.3.

In the ramified case, π_* is surjective on 2-torsion and π^* is injective so it is even more straightforward.

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

We now treat the case of cyclic covers C_q for odd primes q, writing τ 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 $p > \max\{q, (R_q - 1)(q - 1) + 1\}$, then*

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

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

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 ζ_q to τ. Therefore $\ker(1-\tau)$ on $\mathrm{Prym}(\pi)$ has size $q^{2(g_X - g_B)/(q-1)} = q^{2(g_B + R_q - 1)}$ and so $\ker(1-\tau)^{2j}$ has size $q^{2j\cdot(g_B + R_q - 1)}$.

Note that $\pi^* J_B[q] \leq \ker(1-\tau)|_{\mathrm{Prym}(\pi)}$, so for $1 \leq i \leq q-1$ we have a space H such that

$$\pi^* J_B[q] \cong H \leq \ker((1-\tau)^i \circ \pi^*)/\ker((1-\tau)^{i-1} \circ \pi^*)$$

as wild inertia representations. The first conclusion now follows by writing

$$J_X[q] \cong \bigoplus_{i=1}^{q} \ker((1-\tau)^i \circ \pi^*)/\ker((1-\tau)^{i-1} \circ \pi^*),$$

noticing that $\ker((1-\tau)^q \circ \pi^*)/\ker((1-\tau)^{q-1} \circ \pi^*) = J_X[q]/\ker(\pi_*)[q] \cong \pi_*(J_X[q])$ and applying Lemma 3.3.

We have shown $n_{\mathrm{wild}}(X^{\mathbb{1}+\sum_i \rho_i}) = n_{\mathrm{wild}}(X^{q\cdot\mathbb{1}})$, where the ρ_i are the non-trivial irreducibles, so we conclude by Lemma 3.11. □

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 4.3. *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. We have, for $p \nmid n$, $p > \max_{q|n}\{q, (R_q - 1)(q - 1) + 1\}$,*

$$\sum_{\rho' \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q})\cdot\rho} n_{\mathrm{wild}}(X^{\rho' - \mathbb{1}}) = 0,$$

where ρ is any irreducible C_n-representation.

Proof. We go by induction on n.

Choose prime $q \mid n$ and $C_q \leq C_n$. Writing ρ'_i for the non-trivial irreducible C_q-representations we have

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

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 $R_q \cdot n/q$.

Decomposing $\mathrm{Ind}_{C_q}^{C_n}(\sum_i \rho_i' - (q-1)\cdot \mathbb{1})$ into irreducibles, we have that each irreducible C_n-representation appears with the same multiplicity as its conjugates. By applying the inductive hypothesis to any non-faithful representations, noting that we can pass to quotients because the quotient cover will have at most R_q points with ramification index divisible by q, we obtain a relation

$$a \cdot \sum_{\rho \text{ faithful}} n_{\text{wild}}(X^{\rho}) = b \cdot n_{\text{wild}}(X^{\mathbb{1}})$$

for some $a, b \in \mathbb{Z}$. Frobenius reciprocity shows that $a \neq 0$ and we conclude that $b/a = \phi(n) = \#(\mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cdot \rho)$ for ρ faithful because all the relations used are of the form $n_{\text{wild}}(X^{\eta}) = 0$, where η is a degree 0 character. $\square$

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.

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 ε for the sign representation and, as always, $\mathbb{1}$ for the trivial irreducible representation of S_n.

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*

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

We first give some discussion of the special case $n = 3$.

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 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.

$$\begin{tikzcd}
& X \arrow[dl, "\pi_{X,C}"'] \arrow[dd, "\pi_{X,B}"] \arrow[dr, "\pi_{X,D}"] & \\
C = X/C_2 \arrow[dr, "\pi_{C,B}"'] & & D = X/C_3 \arrow[dl, "\pi_{D,B}"] \\
& B = X/S_3 &
\end{tikzcd}$$

By Proposition 4.2 we have $n_{X,\text{wild}} = 3 \cdot n_{D,\text{wild}}$ for $p > \max\{3, 2(R_3 - 1)\}$, where R_3 is the number of points with ramification index divisible by 3. We obtain a relation $n_{\mathrm{wild}}(X^{F_3}) = n_{\mathrm{wild}}(X^{\mathbb{1} + \det F_3})$, which is the case $n = 3$ of Theorem 5.2. Moreover, 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 the special case $R_3 = 1$ and $B = \mathbb{P}^1$, this yields an isomorphism of G_K-modules

$$(\dagger) \qquad (1-\tau) \circ \pi^*_{X,C} J_C[3] \xrightarrow{\sim} \pi^*_{X,D} J_D[3],$$

and we identify $\pi^*_{X,D} J_D[3]$ with $J_D[3]$ because $\pi_{X,D}$ is ramified in this case.

Remark 5.3. In the case of an elliptic curve $C : y^2 = x^3 + ax + b$, $a \neq 0$ with $B = \mathbb{P}^1_y$, 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 [6, Lemma 6.9 + Remark 6.10], where they study the kernel of an isogeny $J_C^2 \times J_D \to J_X \times J_B^2$. ♢

Remark 5.4. 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 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 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 Galois and representation-theoretic lemmata which will be required.

Lemma 5.5. *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 π 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_{n-1}° correspond to the orbits of $\{1, \ldots, n\}$ under the action of the decomposition group at $\mathfrak{P}$. The assumption that $X/S_{n-1}^\circ \to B$ 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. [15, §9.2]).

Lemma 5.6. *Given a virtual character χ of S_n with degree 0, there exists some integers a_i, not-necessarily-distinct cyclic subgroups H_i and virtual characters Θ_i of the form*

$$\Theta_i = \sum_{\rho' \in \mathrm{Gal}(\mathbb{Q}(\rho)/\mathbb{Q}) \cdot \rho} (\rho' - \mathbb{1}_{H_i}),$$

where ρ 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 Θ 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 $\langle \operatorname{Res}_H \chi, \Theta \rangle = 0$ for all characters Θ of H of the above form, by assumption. Therefore $\operatorname{Res}_H \chi = 0$ because these Θ obviously generate the set of rational characters of H with degree 0. Thus χ 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 5.7. *Let $C_2 \leq S_n$ be generated by a transposition. We have*

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

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

For general n, restricting to S_{n-1}° gives $\operatorname{Res}_{S_{n-1}^{\circ}} F_n = F_{n-1} + \mathbb{1}_{S_{n-1}^{\circ}}$ 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 Θ_i as in Lemma 5.6 such that

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

If we choose H_i to contain no transposition, then $n_{\mathrm{wild}}(X^{\operatorname{Ind}_{H_i}^{S_n} \Theta_i}) = 0$ by Lemma 5.5. The cycle types which generate subgroups containing transpositions are transpositions themselves along with the product of cycles of odd lengths with a transposition.

The case of transpositions is dealt with by Lemma 5.7. For the case of the product of a transposition with cycles of odd length, write $2m$ for the order of such a permutation. Now, as in the proof of Lemma 5.7, $\operatorname{Res}_{C_2} F = (n-2) \cdot \mathbb{1}_{C_2} + \varepsilon_{C_2}$ so $\operatorname{Res}_{C_2 \times C_m} F$ is a sum of $(n-1)$ irreducibles lifted from C_m and one irreducible representation which restricts to the ε_{C_2} on C_2, which must be $\operatorname{Res}_{C_2 \times C_m} \varepsilon$ because F is rational. Therefore $\operatorname{Res}_{C_{2m}}(F - \varepsilon - (n-2) \cdot \mathbb{1})$ is in the space generated by characters lifted from C_m, so we are done.

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. This makes the details slightly more cumbersome, but the conclusion is the same. □

Remark 5.8. 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 divisible by 3, in which case we have equality, for example, between the wild conductor exponents at 2 also.

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 exponents at each such q. ♢

Remark 5.9. It is a result of credited by Fulton to Severi ([7, 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 an 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}° 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 (=[4, 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.*

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

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. $\diamondsuit$

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 [4, 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. We think of the points in R_h close to r_0 as a 'cluster' of e_i points. By continuity of the W_K-action, there is an orbit of clusters mirroring the orbit of r_0. Supposing that the orbit of r contains more than one point in any of these clusters leads to a contradiction because $|W_K \cdot r_0| < |W_K \cdot r| \leq |W_K \cdot r_0| \cdot (p-1)$, but these quantities cannot all 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. $\square$

We now consider a curve given by a smooth affine model $C/K : f(x, y) = 0$, in which setting we prove our main theorem. We need the following lemma to reduce to the case of Theorem 5.2.

Lemma 6.4. *Suppose $C/K : f(x, y) = a_n(y)x^n + a_{n-1}(y)x^{n-1} + \ldots + a_0(y) = 0$ is smooth away from infinity. We can choose $\widetilde{f}(x, y)$ arbitrarily close to f (in the sense that their coefficients are close as polynomials in y) such that $\widetilde{C}/K : \widetilde{f}(x, y) = 0$ satisfies $g_C = g_{\widetilde{C}}$, and projection onto y gives a simply branched cover $\widetilde{C} \to \mathbb{P}^1$, except possibly above infinity.*

Proof. Write $\widetilde{f}_{\boldsymbol{\varepsilon}}(x, y) = f(x, y) + \sum_{i=0}^{n-1} \varepsilon_i x^i$, where $\boldsymbol{\varepsilon} = (\varepsilon_0, \ldots, \varepsilon_{n-1})$, noting that perturbing in this way will not affect the behaviour at infinity. Write $g_{\boldsymbol{\varepsilon}}$ for the factor of $\mathrm{disc}_x f$ coming from ramification above finite points, so $\mathrm{disc}_{\varepsilon_1} \mathrm{disc}_x g_{\boldsymbol{\varepsilon}}$ is a polynomial in the ε_i with coefficients in the a_i. We can choose the ε_i such that this discriminant is not the zero function in y and the ε_i are small with respect to v_K because $g_{\boldsymbol{\varepsilon}}$ clearly has no factors which depend only on y. Note that if $g_{\boldsymbol{\varepsilon}}$ has a square factor for all ε_i then $\mathrm{disc}_{\varepsilon_i} \mathrm{disc}_x f(x, y) = 0$, so we are done. □

Finally, we are able to show Theorem 1.4.

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

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

Proof. Consider the map $C \to \mathbb{P}^1$ given by projection onto y. When this is simply branched away from one point and has S_n-Galois closure, we are done by Theorem 5.2 and Theorem 6.1.

To reduce to this case, we first assume that $C : f(x, y) = 0$ is smooth at infinity. Now perturb the equation $f(x, y) = 0$ as in Lemma 6.4, noting that we can ensure that $\mathrm{Gal}(\widetilde{f}) \cong S_n$ as a polynomial over $\overline{K}(y)$ using the same perturbations described: if this is not the case, then $\mathrm{Gal}(\widetilde{f}_{\boldsymbol{\varepsilon}}(x, y_0)) \lneqq S_n$ for any choice of y_0, but now fix y_0 and choose $\boldsymbol{\varepsilon}'$ still small with respect to v_K such that $\mathrm{Gal}(\widetilde{f}_{\boldsymbol{\varepsilon}'}(x, y_0)) \cong S_n$, which is easily done.

We may then use Lemma 6.3 and the local constancy of wild conductor exponents [8, Theorem 5.1(1)]. The latter theorem applies because perturbing in the described way yields an ℓ-adic family of curves of constant genus.

When the C is not smooth at infinity, pass to the normalisation of the discriminant curve D (i.e. divide by square factors), which has the same wild conductor exponent as C. Conclude by noticing that the additional factor coming from $(1 : 0 : 0)$ in $\mathrm{disc}_x f$ is a power of y and the factor coming from points $(x_i : 1 : 0)$ is a product of K-rational polynomials of degree at most n, so neither contribute to $w_K(\mathrm{disc}_x f)$. □

Remark 6.6. One could replace infinity by any K-rational point of $\mathbb{P}^1$, provided that one can perturb the equation of C in such a way as to fix this point. In practice, one would simply make a change of variables in this situation. ◇

Corollary 6.7. *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*

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

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 [5, 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 $(u_1, \ldots, u_7) \in \overline{k}^7$ 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 [10] label 1744.a.1744.1 which has model

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

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 using Magma we find that there are none. Indeed, one can check that there are only 78 solutions to this system of equations over $\overline{\mathbb{Q}}$. $\diamondsuit$

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 three sets of tuples $(u_1, \ldots, u_7) \in \overline{k}^7$, $(v_1, \ldots, v_6) \in \overline{k}^6$ and $(w_1, \ldots, w_5) \in \overline{k}^5$ respectively satisfying the equalities*

$$\begin{aligned} F(x) &= (u_4x^3 + u_3x^2 + u_2x + u_1)^2 - u_7(x^2 + u_6x + u_5)^3 \\ &= (v_4x^3 + v_3x^2 + v_2x + v_1)^2 - v_6(x + v_5)^3 \\ &= (w_4x^3 + w_3x^2 + w_2x + w_1)^2 - w_5. \end{aligned}$$

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 two 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 $(a_3x^3 + a_2x^2 + a_1x + a_0)^2 - F(x)$, for some a_i, with divisor $3(X_1) + 3(X_2) - 6(\infty)$ a cube (e.g. [11, Lemma 1]). 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. □

The troublesome cases for which the original result fails are those curves admitting degree 3 covers of $\mathbb{P}^1$ with discriminant curve of genus at most 1, examples of which are mentioned in [3, Example 2]. We see this from the following easily-proved lemma.

Lemma A.3. *Let C/k be a genus 2 curve admitting a degree 3 cover of $\mathbb{P}^1_k$. There is a divisor $\mathcal{D}$ on C corresponding to a non-zero element of $J_C[3]$ of the form*

$$\mathcal{D} = (P) - (\infty_1),$$

where ∞_1 is one of the two points at infinity of C, if and only if the corresponding discriminant curve D has genus strictly less than 2.

References

[1] Indranil Biswas, Manish Kumar, and A. J. Parameswaran. Genuinely ramified maps and monodromy. arXiv: 2401.08526, 2024.

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

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

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

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

[6] Vladimir Dokchitser, Holly Green, Alexandros Konstantinou, and Adam Morgan. Parity of ranks of Jacobians of curves. arXiv: 2211.06357v2, 2024.

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

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

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

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

[11] Elvira Lupoian. Three-Torsion Subgroups and Conductors of Genus 3 Hyperelliptic Curves. arXiv: 2210.02225v3, 2022.

[12] Elvira Lupoian. Two-torsion subgroups of some modular Jacobians. *International Journal of Number Theory*, to appear.

[13] Elvira Lupoian and James Rawson. 3-torsion subgroups of Jacobians of plane quartics. arXiv: 2401.13577, 2024.

[14] David Mumford. Prym varieties I. In *Contributions to Analysis*, pages 325–350. Academic Press, 1974.

[15] 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.

[16] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88(3):492–517, 1968.
[17] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer–Verlag, 1994.
[18] Douglas Ulmer. Conductors of ℓ-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