

# JOURNAL

de Théorie des Nombres  
de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Matthew BISATT

**Root number of the Jacobian of  $y^2 = x^p + a$**

Tome 34, n° 2 (2022), p. 575-582.

<https://doi.org/10.5802/jtnb.1217>

© Les auteurs, 2022.



Cet article est mis à disposition selon les termes de la licence  
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.  
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du  
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

# Root number of the Jacobian of $y^2 = x^p + a$

par MATTHEW BISATT

RÉSUMÉ. Soit  $C/\mathbb{Q}$  une courbe hyperelliptique donnée par un modèle affine de la forme  $y^2 = x^p + a$ . Nous déterminons le signe de la Jacobienne de  $C$ , en particulier nous nous concentrons sur le signe local en  $p$ , où  $C$  est sauvagement ramifiée.

ABSTRACT. Let  $C/\mathbb{Q}$  be a hyperelliptic curve with an affine model of the form  $y^2 = x^p + a$ . We explicitly determine the root number of the Jacobian of  $C$ , with particular focus on the local root number at  $p$  where  $C$  has wild ramification.

## 1. Global case

Let  $A/\mathbb{Q}$  be an abelian variety. One of the consequences of the famed Birch and Swinnerton-Dyer conjecture is that the parity of the rank of  $A/\mathbb{Q}$  should be controlled by the expected sign in its functional equation. The expected sign is known as the (global) root number of  $A$  and denoted by  $W(A/\mathbb{Q})$ ; the parity conjecture states that  $W(A/\mathbb{Q}) = (-1)^{\text{rank } A(\mathbb{Q})}$ .

Root numbers of elliptic curves are completely understood, but the same cannot be said in higher dimensions. Whilst root numbers only conjecturally control the rank, current computer algebra packages are often unable to compute either the  $L$ -function or rank explicitly in high dimension; when these computations are coupled with the root number however, one is more likely to be able to predict the rank exactly. For example, a root number calculation may predict that the Jacobian of a curve has rank 0, and thus make the curve more amenable to Chabauty-type arguments since one generally needs to know explicit generators of a finite index subgroup to apply them.

The author has previously described the root number when  $A$  has everywhere tame reduction [2], with an explicit description when  $A$  arises as the Jacobian of a hyperelliptic curve. The purpose of this note is to compute the root number of the Jacobian of a hyperelliptic curve of the form  $y^2 = x^p + a$  when  $p$  is an odd prime. We concentrate on the case when  $a$  is not a  $p$ -th power in  $\mathbb{Q}_p$  although this restriction is not necessary (see

---

Manuscrit reçu le 19 février 2021, révisé le 13 août 2021, accepté le 29 octobre 2021.

2020 *Mathematics Subject Classification*. 11G20, 11G40.

*Mots-clefs*. Root numbers, hyperelliptic curves.

This work was funded by the Heilbronn Institute for Mathematical Research.

Remark 1.3). The main theoretical contributions of this paper are that we extend a result of Kobayashi’s to deal with the wild ramification at  $p$  and also give an approach to treat the reduction at 2 where one cannot use the theory of cluster pictures of hyperelliptic curves to determine the Galois representation.

We will not list the various properties of root numbers that we use here, but instead refer the reader to [2, §2] for an overview or [11, §3] for more details.

For a prime  $p$ , we write  $v_p$  for the  $p$ -adic valuation,  $\left(\frac{*}{p}\right)$  for the Legendre symbol and  $(-, -)_{\mathbb{Q}_p}$  for the Hilbert symbol at  $p$ .

**Theorem 1.1.** *Fix  $0 \neq a \in \mathbb{Z}$  and an odd prime  $p$ . Let  $\mathcal{C}_a/\mathbb{Q}$  be the hyperelliptic curve  $y^2 = x^p + a$  and let  $J_a$  be its Jacobian. Assume that  $a$  is not a  $p$ -th power in  $\mathbb{Q}_p$  and let  $a' = 2^{-v_2(a)}a$ .*

- (1) Let  $W_2 = \begin{cases} \left(\frac{2}{p}\right) & \text{if } v_2(a) \text{ is even, } p \nmid v_2(4a), \text{ and } a' \equiv 1 \pmod{4}, \\ \left(\frac{-1}{p}\right) & \text{if } a' \equiv 3 \pmod{4}, \\ 1 & \text{else.} \end{cases}$
- (2) Assume there exists a model of  $\mathcal{C}_a$  of the form  $y^2 = g(x)$ , where  $p \nmid v_p(g(0))$ . Let  $a_0 = g(0)$  and let  $\Delta_g$  be the discriminant of  $g$ . Define

$$W_p = - \left(\frac{-2}{p}\right) (a_0(p-1)v_p(a_0), \Delta_g)_{\mathbb{Q}_p} \left(\frac{-1}{p}\right)^{\frac{1+v_p(\Delta_g)}{2}}.$$

Write

$$S_1 = \{\text{primes } \ell \mid a : \ell \notin \{2, p\}, v_\ell(a) \text{ odd}\},$$

$$S_2 = \{\text{primes } \ell \mid a : \ell \notin \{2, p\}, p \nmid v_\ell(a), v_\ell(a) \text{ even}\}.$$

Then the global root number of  $J_a$  is

$$W(J_a/\mathbb{Q}) = W_2 W_p \left(\frac{-1}{p}\right) \prod_{\ell \in S_1} \left(\frac{-1}{\ell}\right)^{\frac{p-1}{2}} \prod_{\ell \in S_2} \left(\frac{\ell}{p}\right).$$

**Remark 1.2.** As in the elliptic curve setting, a suitable model for  $\mathcal{C}_a$  always exists; see [7, Proposition 5.1b] for the genus two case or [8, Proposition III.1.2] for the case under consideration here. In practice, it appears that taking  $g(x) = f(x + r)$  for some  $r \equiv -a \pmod{p}$  suffices to obtain a suitable model.

**Remark 1.3.** The assumption that  $a$  is not a  $p$ -th power in  $\mathbb{Q}_p$  is only used to compute the local root number  $W_p = W(J_a/\mathbb{Q}_p)$ . If  $a$  is a  $p$ -th power in  $\mathbb{Q}_p$  then one can still compute that the inertia representation at  $p$  is tamely ramified and isomorphic to  $\gamma \otimes \mathbb{C}[C_{p-1}]$ , where  $\gamma$  is a faithful character of  $C_{2(p-1)}$ , and then deduce the root number by [1, §11, §13]. We choose to omit the result here in the interest of brevity.

*Proof.* Note that the discriminant of  $\mathcal{C}_a$  is  $(-1)^{\frac{p-1}{2}} 2^{2(p-1)} p^p a^{p-1}$  and hence

$$W(J_a/\mathbb{Q}) = W(J_a/\mathbb{R})W(J_a/\mathbb{Q}_2)W(J_a/\mathbb{Q}_p) \prod_{\ell|a, \ell \neq 2, p} W(J_a/\mathbb{Q}_\ell).$$

Moreover, one has that  $W(J_a/\mathbb{R}) = (\frac{-1}{p})$  (see for example [9, Lemma 2.1]).

Now suppose that  $\ell \neq p$  is an odd prime. We will use the theory of clusters to compute the corresponding inertia representation and refer the reader to the user's guide [1] for the relevant definitions and theorem statements. The set of roots is  $\mathcal{R} = \{\zeta_p^j \sqrt[p]{-a} \mid 0 \leq j \leq p-1\}$ , for  $\zeta_p$  a primitive  $p$ -th root of unity; this is the only proper cluster of  $\mathcal{C}_a$  and has depth  $\frac{v_\ell(a)}{p}$ . Moreover, inertia acts on  $\mathcal{R}$  through a  $C_p$ -quotient and the action is trivial if and only if  $p \mid v_\ell(a)$ .

If  $p \nmid v_\ell(a)$ , then  $H_{\text{ét}}^1(J_a/\mathbb{Q}_\ell, \overline{\mathbb{Q}}_2)$  decomposes as an inertia representation into  $p-1$  characters of order either  $2p$  if  $v_\ell(a)$  is odd and order  $p$  otherwise. The corresponding local root number is then either  $(\frac{-1}{\ell})^{\frac{p-1}{2}}$  or  $(\frac{\ell}{p})$  respectively by [1, Theorem 13.4]. On the other hand, if  $p \mid v_\ell(a)$ , then  $H_{\text{ét}}^1(J_a/\mathbb{Q}_\ell, \overline{\mathbb{Q}}_2)$  decomposes into  $p-1$  characters of order either  $2$  if  $v_\ell(a)$  is odd and order  $1$  otherwise; in this case the local root number is then  $(\frac{-1}{\ell})^{\frac{p-1}{2}}$  or  $1$  respectively.

Next we compute the local root number at  $2$ , for which we can no longer apply the cluster machinery. First suppose that  $v_2(a) = 2k$  is even and  $a' = a2^{-2k} \equiv 1 \pmod{4}$ . Using the substitution  $(x, y) \mapsto (x, y+2^k)$ , we change our model for  $\mathcal{C}_a/\mathbb{Q}_2$  to  $y^2 + 2^{k+1}y = x^p + 4^k(a' - 1)$ . Let  $\pi$  be a fixed choice of  $\sqrt[2]{2}$  in some algebraic closure of  $\mathbb{Q}_2$  and let  $L = \mathbb{Q}_2(\pi^{2(k+1)})$ . Consider the base change  $\mathcal{C}_L$  of  $\mathcal{C}_a$  to  $L$  with the substitution  $x = \pi^{2(k+1)}X, y = 2^{k+1}Y$ ; this gives us a model for  $\mathcal{C}_L$  as  $Y^2 + Y = X^p + \frac{a'-1}{4}$  which has good reduction over  $L$ . Now  $L = \mathbb{Q}_2$  if and only if  $p \mid (k+1)$ ; in this case the root number is  $1$ . If  $p \nmid (k+1)$ , then  $L = \mathbb{Q}_2(\pi)$  and using the lift-act-reduce procedure of [5, Theorem 1.5] (this example is analogous to Example 1.9 of *loc. cit.*) one can moreover see that the inertia representation is  $\mathbb{C}[C_p] \oplus \mathbb{1}$  and hence the local root number is  $W(J_a/\mathbb{Q}_2) = (\frac{2}{p})$ .

The remaining cases at  $2$  are quadratic twists of the one above so we will make use of the well-known formula

$$W(A/\mathbb{Q}_\ell)W(A^D/\mathbb{Q}_\ell) = W(A/\mathbb{Q}_\ell(\sqrt{D}))\chi_D(-1)^{\dim A},$$

where  $A/\mathbb{Q}_\ell$  is an abelian variety,  $A^D$  its quadratic twist by  $D$ , and  $\chi_D$  is the quadratic character of  $\text{Gal}(\mathbb{Q}_\ell(\sqrt{D})/\mathbb{Q}_\ell)$ .

Note that if  $\tilde{a} \equiv 1 \pmod{4}$ , then  $\mathcal{C}_a$  is a quadratic twist of a curve of the form  $\mathcal{C}_{2^{2k}\tilde{a}}$  for some  $D \in \{-1, 2, -2\}$ ; if  $a' = 2^{-v_2(a)}a$ , then the required quadratic twist is given by the squarefree part of  $(-1)^{\frac{a'-1}{2}} 2^{v_2(a)}$ .

Since  $\mathcal{C}_{2^{2k}\bar{a}}$  obtains good reduction over  $L$  which has ramification degree dividing  $p$  and  $\mathbb{Q}_2(\sqrt{D})/\mathbb{Q}_2$  is ramified of degree coprime to  $p$ , one has that  $W(J_{2^{2k}\bar{a}}/\mathbb{Q}_2) = W(J_{2^{2k}\bar{a}}/\mathbb{Q}_2(\sqrt{D}))$  (note it does not matter whether  $L = \mathbb{Q}_2$  here). Hence  $W(\text{Jac}(\mathcal{C}_{2^{2k}\bar{a}}^D)/\mathbb{Q}_2) = \chi_D(-1)^{\frac{p-1}{2}}$ . One can compute via class field theory that  $\chi_{-1}(-1) = \chi_{-2}(-1) = -1$  and  $\chi_2(-1) = 1$ , and hence the local root number  $W_2 = W(J_a/\mathbb{Q}_2)$  follows.

Now let  $\ell = p$  and consider the model change to  $y^2 = g(x)$ . Note that the two torsion field of  $J_a$  is independent of the choice of model and equal to the splitting fields of  $f$  and  $g$ . Since  $a$  is not a  $p$ -th power in  $\mathbb{Q}_p$ ,  $g$  satisfies the hypotheses of Theorem 2.1 and the computation of the local root number  $W_p = W(J_a/\mathbb{Q}_p)$  follows. □

**Remark 1.4.** When  $\ell = 2$ , one could also obtain the inertia representation in the tame case via [4, §1.3].

### 2. Local case at $p$

We now compute the local root number at  $p$ . Our method closely follows that of [6], adapting for higher genus. We first collate the bulk of the notation that we will use throughout this section for ease of reading.

**Notation.** For a finite extension  $F/\mathbb{Q}_p$ , we denote

- $\mathcal{O}_F$      the valuation ring of  $F$ ,
- $v_F$      the normalised valuation of  $F$  so that  $v_F(F^\times) = \mathbb{Z}$ ,
- $\mathbb{F}_F$      the residue field of  $F$ ,
- $q_F$      =  $|\mathbb{F}_F|$  the cardinality of the residue field of  $F$ ,
- $F^{un}$     the maximal unramified extension of  $F$ ,
- $\mathcal{W}(F'/F)$  the Weil group of an extension  $F'/F$ ,
- $\text{Tr}_{F'/F}$  the trace map for a finite extension  $F'/F$ .

For an irreducible squarefree polynomial  $f \in K[x]$  of degree  $p$ , we also define:

- $\mathcal{C}_f$     the hyperelliptic curve  $y^2 = f(x)$ ,
- $\rho_\ell$     the  $\ell$ -adic representation of  $\text{Jac}(\mathcal{C}_f)$  for  $\ell \neq p$ ,
- $\alpha$     a root of  $f$ ,
- $\Delta_f$    the discriminant of  $f$ ,
- $M$     the splitting field of  $f$ ,
- $\sigma$     a fixed element of order  $p$  in the Galois group  $\text{Gal}(M/K)$ ,
- $N$     =  $M(\sqrt{\alpha - \sigma\alpha})$ .

For nonzero complex numbers  $a, b$ , we write  $a \approx b$  if  $ab^{-1} \in \mathbb{C}$  is in the multiplicative group generated by the positive real numbers and the  $p$ -power roots of unity. We are now in a position to state our theorem.

**Theorem 2.1.** *Let  $p$  be an odd prime,  $K/\mathbb{Q}_p$  a finite extension and let  $f \in K[x]$  be a squarefree polynomial of degree  $p$ . Suppose that:*

- (1)  $f$  is irreducible;
- (2) the valuation of the discriminant of  $f$ ,  $v_K(\Delta_f)$ , is coprime to  $p - 1$ ;
- (3) the splitting field  $M$  of  $f$  has degree  $p(p - 1)$ ;
- (4)  $p \nmid v_K(a_0)$  where  $a_0 = f(0)$ .

Then, for the hyperelliptic curve  $\mathcal{C}_f : y^2 = f(x)$ , the local root number is

$$W(\text{Jac}(\mathcal{C}_f)/K) = - \left( \frac{-2}{q_K} \right) (a_0(p - 1)v_K(a_0), \Delta_f)_K \left( \frac{-1}{q_K} \right)^{\frac{1+v_K(\Delta_f)}{2}}.$$

We will implicitly assume these hypotheses from now on in order to prove this theorem through a series of lemmas.

**Proposition 2.2.**

- (1) Let  $\sigma$  be an element of order  $p$  of  $\text{Gal}(M/K) \cong C_p \rtimes C_{p-1}$  and let  $N = M(\sqrt{\alpha - \sigma\alpha})$ . Then  $\rho_J$  is a faithful representation of the Weil group  $\mathcal{W}(N^{un}/K)$ .
- (2) Let  $H \subset M$  be such that  $[H : K] = p - 1$ . Then  $\rho_J = \text{Ind}_{H/K} \chi$  is the induction of a character  $\chi$  from  $\mathcal{W}(N^{un}/H)$ ;
- (3) The conductor exponent of  $\chi$ ,  $a(\chi)$ , is even.

*Proof.* (1)–(2) follow from Proposition 2.2 and §5.1 of [3].

Let’s now prove (3). Note that  $a(\rho_J) = v_K(\Delta_{K(\alpha)/K})$ , where  $\Delta_{K(\alpha)/K}$  is the relative discriminant of the valuation ring of  $K(\alpha)$ , by [3, §6]; we claim this is odd. Since the discriminant of the lattice  $\mathcal{O}_K[\alpha]$  is equal to  $\Delta_f$  and has square index inside the valuation ring,  $v_K(\Delta_{K(\alpha)/K}) \equiv v_K(\Delta_f) \pmod{2}$  from which the claim follows. By the conductor exponent of induced representations formula [10, p. 101],  $a(\chi)$  is even.  $\square$

We now fix an additive character  $\psi$  of  $K$  with conductor  $-1$  such that  $\psi(x) = \chi(\sigma)^{-\text{Tr}_{\mathbb{F}_K/\mathbb{F}_p}(\bar{x})}$  whenever  $x \in \mathcal{O}_K$ , where  $\text{Tr}_{\mathbb{F}_K/\mathbb{F}_p}$  is the trace map from  $\mathbb{F}_K$  to  $\mathbb{F}_p$  and  $\bar{x}$  is the image of  $x$  in  $\mathbb{F}_K$ . We further let  $\psi_H$  be the composition of  $\psi$  with the trace map  $\text{Tr}_{H/K}$ , also of conductor  $-1$ . We also choose an arithmetic Frobenius element  $\text{Frob}$  of  $\mathcal{W}(N^{un}/N) \subset \mathcal{W}(N^{un}/K)$  and extend  $\sigma$  to  $\mathcal{W}(N^{un}/K)$  by imposing that it acts trivially on  $K^{un}$  and  $\sqrt{\alpha - \sigma\alpha}$ .

**Lemma 2.3.** *Let  $\text{sign}_{H/K}$  be the nontrivial quadratic character of  $\text{Gal}(H/K)$ . Then*

$$W(\rho_J, \psi) = \left( \frac{-2}{q_K} \right) W(\text{sign}_{H/K}, \psi_H)W(\chi, \psi_H).$$

*Proof.* For  $F \subset N$ , let  $\mathbb{1}_F$  denote the trivial character of  $\mathcal{W}(N^{un}/F)$ . Since root numbers are inductive in degree 0, one has  $W(\text{Ind}_{H/K} \chi, \psi) = W(\text{Ind}_{H/K} \mathbb{1}_H, \psi)W(\chi, \psi_H)$ .

We now compute  $W(\text{Ind}_{H/K} \mathbb{1}_H, \psi)$ . Let  $\mu$  be a faithful character of  $\mathcal{W}(N^{un}/K)/\mathcal{W}(N^{un}/H) \cong \text{Gal}(H/K) \cong C_{p-1}$ . Then

$$\text{Ind}_{H/K} \mathbb{1}_H = \mathbb{1}_K \oplus \text{sign}_{H/K} \oplus \bigoplus_{1 \leq j < \frac{p-1}{2}} (\mu^j \oplus \mu^{-j}),$$

and hence

$$W(\text{Ind}_{H/K} \mathbb{1}, \psi) = W(\mathbb{1}_K, \psi)W(\text{sign}_{H/K}, \psi) \prod_{1 \leq j < \frac{p-1}{2}} \mu^j(-1).$$

Now  $W(\mathbb{1}_K, \psi) = 1$  and  $\mu^j(-1) = 1 \Leftrightarrow q_K \equiv 1 \pmod{2 \frac{p-1}{\gcd(j, p-1)}}$  by [2, Lemma 3.8]. If  $q_K$  is an even power of  $p$ , then this is always satisfied since  $2(p-1)$  divides  $(q_K - 1)$ . On the other hand, if  $q_K$  is an odd power of  $p$ , then this congruence is satisfied if and only if  $j$  is even so it suffices to count the number of odd integers in the range  $1 \leq j < \frac{p-1}{2}$ ; the parity of this is precisely given by the Legendre symbol  $(\frac{-2}{p})$ .  $\square$

**Remark 2.4.** One of our running assumptions is that the splitting field of  $f$  has degree  $p(p-1)$  over  $K$ ; the preceding lemma is the only place we made use of this fact since this implies that  $H/K$  is a cyclic Galois extension.

We briefly generalise Propositions 5.7 and 5.13 of [6] now.

**Lemma 2.5.** *Let  $\bar{\mathcal{C}}/\mathbb{F}_q : y^2 = x^p - x$  and let  $\overline{\text{Frob}}$  be the Frobenius endomorphism of  $\bar{\mathcal{C}}$  given by  $(x, y) \mapsto (x^q, y^q)$  and let  $\bar{\rho}$  be the endomorphism  $(x, y) \mapsto (x + 1, y)$ . By Albanese functoriality, these descend to endomorphisms of the Jacobian  $\bar{J}$  of  $\bar{\mathcal{C}}$  which we again denote by  $\overline{\text{Frob}}$  and  $\bar{\rho}$ . Then in the endomorphism ring of  $\bar{J}$ , one has*

$$\overline{\text{Frob}} = - \sum_{u \in \mathbb{F}_q^\times} \binom{u}{q} \bar{\rho}^{\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(u)}.$$

*Proof.* By the Hasse–Davenport Theorem, it suffices to prove this when  $q = p$ . Let  $\infty$  denote the point at infinity of  $\bar{\mathcal{C}}$  and embed  $\iota : \bar{\mathcal{C}} \hookrightarrow \bar{J}$  via  $P \mapsto [(P) - (\infty)]$ . Let  $P = (x, y)$ ; it suffices to prove this equality for  $\iota(P)$  since  $\bar{J}$  is generated by the image of  $\iota$ . Using the hyperelliptic involution, we have

$$\left( \overline{\text{Frob}} + \sum_{u \in \mathbb{F}_p^\times} \binom{u}{p} \bar{\rho}^u \right) (\iota(P)) = (x^p, y^p) + \sum_{u \in \mathbb{F}_p^\times} (x + u, \binom{u}{p} y) - p(\infty).$$

One can check that this is the divisor of  $Y - y(X - x)^{\frac{p-1}{2}}$  and hence is trivial on  $\bar{J}$ , which proves the equality.  $\square$

**Proposition 2.6.** *As operators of  $H_{\text{ét}}^1(\mathcal{C}_f/\overline{K}, \mathbb{Q}_\ell)$ , we have an equality*

$$\text{Frob} = - \sum_{u \in \mathbb{F}_K^\times} \left( \frac{u}{q_K} \right) \sigma^{-\text{Tr}_{\mathbb{F}_K/\mathbb{F}_p}(u)}.$$

*Proof.* Note that over  $N$ , the model of  $\mathcal{C}_f$  determined by the substitution  $(x, y) \mapsto ((\alpha - \sigma\alpha)x + \alpha, \sqrt{\alpha - \sigma\alpha^p}y)$  reduces to  $y^2 = x^p - x$  (see [3, Lemma 4.1]). Moreover, one can show via the lift-act-reduce method of [5, Theorem 1.5], that  $\text{Frob}$  and  $\sigma^{-1}$  act on  $H_{\text{ét}}^1(\mathcal{C}_f/\overline{\mathbb{F}}_K, \mathbb{Q}_\ell)$  as  $(x, y) \mapsto (x^{q_K}, y^{q_K})$  and  $(x, y) \mapsto (x+1, y)$  respectively (equivalently use the function field approach of [6, Proposition 5.12]). The Galois module isomorphism of [5, Corollary 1.6] then transfers the operator equality of Lemma 2.5 to  $H_{\text{ét}}^1(\mathcal{C}_f/\overline{K}, \mathbb{Q}_\ell)$ .  $\square$

**Lemma 2.7.** *Let  $G$  be the Gauss sum  $\sum_{u \in \mathbb{F}_K^\times} \left( \frac{u}{q_K} \right) \chi(\sigma)^{-\text{Tr}_{\mathbb{F}_K/\mathbb{F}_p}(u)}$ . Then*

$$W(\chi, \psi_H) \approx (a_0 v_M(\alpha), \Delta_f)_K (-G)^{v_K(\Delta_f)}.$$

*Proof.* First note that  $W(\chi, \psi_H) \approx \chi \left( \frac{-\text{Norm}_{M/H}(\alpha - \sigma\alpha)}{a_0 v_M(\alpha)^p} \right)$  by the proofs of Propositions 4.2 and 5.6 of [6]. The remainder is largely [6, Proposition 5.8].

Note  $\chi|_{K^\times} = \text{sign}_{H/K} \det \rho_J$ . Since  $\det \rho_J$  is an integer power of the cyclotomic character and  $\text{sign}_{H/K}$  is the Hilbert symbol  $(-, \Delta_f)_K$ , we have  $\chi(a_0 v_M(\alpha)^p) \approx (a_0 v_M(\alpha)^p, \Delta_f)_K = (a_0 v_M(\alpha), \Delta_f)_K$ .

Let  $\beta = -\text{Norm}_{M/H}(\alpha - \sigma\alpha)$ . We now claim that  $v_H(\beta) = v_K(\Delta_f)$ . Since  $\mathcal{C}_f$  has potentially good reduction,  $v_M(\sigma^i \alpha - \sigma^j \alpha) = v_M(\alpha - \sigma\alpha)$  whenever  $\sigma^i \neq \sigma^j$  by [1, Theorem 5.3]. Hence  $v_M(\Delta_f) = p(p-1)v_M(\alpha - \sigma\alpha) = p(p-1)v_H(\text{Norm}_{M/H}(\alpha - \sigma\alpha))$ . The claim follows since  $M/K$  is totally ramified of degree  $p(p-1)$ .

Observe that  $\beta = \text{Norm}_{N/H}(\sqrt{\alpha - \sigma\alpha})$  is a norm from  $N$  and so by Proposition 2.6 with the proof of [6, Proposition 5.8],  $\chi(\beta) = \chi(\text{Frob}^{v_H(\beta)}) = (-G)^{v_K(\Delta_f)}$ .  $\square$

Finally, we can amalgamate these results to prove Theorem 2.1.

*Proof of Theorem 2.1.* By direct computation,  $W(\text{sign}_{H/K}, \psi) \approx G$ . Moreover,  $W(\rho_J, \psi) \approx -\left(\frac{-2}{q_K}\right)(a_0 v_M(\alpha), \Delta_f)_K (-G)^{1+v_K(\Delta_f)}$  by Lemmas 2.3 and 2.7, and  $v_M(\alpha) = (p-1)v_K(a_0)$ . Since  $v_K(\Delta_f)$  is odd and  $G^2$  is real with  $\text{sign}\left(\frac{-1}{q_K}\right)$  we get the result up to  $\approx$  a priori; the equality follows since both sides are  $\pm 1$ .  $\square$

**Acknowledgments.** The author thanks Tim Dokchitser for his suggestion when  $\ell = 2$ , Nirvana Coppola for answering questions on her paper and the referees for their comments.



## References

- [1] A. J. BEST, L. A. BETTS, M. BISATT, R. VAN BOMMEL, V. DOKCHITSER, O. FARAGGI, S. KUNZWEILER, C. MAISTRET, A. MORGAN, S. MUSELLI & S. NOWELL, “A user’s guide to the local arithmetic of hyperelliptic curves”, *Bull. Lond. Math. Soc.* **54** (2022), no. 3, p. 825-867.
- [2] M. BISATT, “Explicit root numbers of abelian varieties”, *Trans. Am. Math. Soc.* **372** (2019), no. 11, p. 7889-7920.
- [3] N. COPPOLA, “Wild Galois representations: a family of hyperelliptic curves with large inertia image”, <https://arxiv.org/abs/2001.08287>, to appear in *Math. Proc. Camb. Philos. Soc.*, 2022.
- [4] T. DOKCHITSER, “Models of curves over discrete valuation rings”, *Duke Math. J.* **170** (2021), no. 11, p. 2519-2574.
- [5] T. DOKCHITSER, V. DOKCHITSER & A. MORGAN, “Tate module and bad reduction”, *Proc. Am. Math. Soc.* **149** (2021), no. 4, p. 1361-1372.
- [6] S.-I. KOBAYASHI, “The local root number of elliptic curves with wild ramification”, *Math. Ann.* **323** (2002), no. 3, p. 609-623.
- [7] Q. LIU, “Modèles minimaux des courbes de genre deux”, *J. Reine Angew. Math.* **453** (1994), p. 137-164.
- [8] L. MELNINKAS, “On local root numbers of abelian varieties”, PhD Thesis, Université de Strasbourg (France), 2021, <https://hal.archives-ouvertes.fr/tel-03258699v2>.
- [9] M. SABITOVA, “Root numbers of abelian varieties”, *Trans. Am. Math. Soc.* **359** (2007), no. 9, p. 4259-4284.
- [10] J.-P. SERRE, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer, 1979.
- [11] J. TATE, “Number theoretic background”, in *Automorphic Forms, Representations and L-Functions*, Proceedings of Symposia in Pure Mathematics, vol. 33-2, American Mathematical Society, 1979, p. 3-26.

Matthew BISATT  
Fry Building  
University of Bristol  
Bristol, BS8 1UG, UK  
*E-mail:* [matthew.bisatt@bristol.ac.uk](mailto:matthew.bisatt@bristol.ac.uk)  
*URL:* <https://sites.google.com/view/mbisatt/>